П/з №11. Агрегация каналов, Etherchannel. Резервирование FHRP. Балансировка нагрузки.

Современные компьютерные сети являются основой для функционирования практически всех сфер деятельности — от корпоративных систем до глобальных интернет-сервисов. С увеличением объема передаваемых данных и требований к отказоустойчивости сетей, перед сетевыми инженерами встают задачи обеспечения высокой производительности, надежности и эффективного использования ресурсов.

Одной из ключевых проблем является необходимость увеличения пропускной способности каналов связи без значительных затрат на замену оборудования. Более того, критически важные сетевые узлы, например шлюзы, должны быть защищены от сбоев. Агрегация каналов позволяет распределить нагрузку на несколько каналов, избегая ситуации, когда одни устройства/каналы перегружены, а другие простаивают.

Агрегация каналов — это технология, которая позволяет объединить несколько физических каналов в один логический. Логический канал, созданный в результате агрегации, рассматривается сетевыми устройствами как единый интерфейс. Этот логический канал позволяет повысить производительность сети без необходимости замены существующего оборудования.

Агрегация каналов имеет следующие преимущества:

1. **Увеличение пропускной способности**: объединение нескольких каналов позволяет увеличить общую пропускную способность сети.
2. **Резервирование**: если один из физических каналов выходит из строя, трафик автоматически перераспределяется на оставшиеся каналы.
3. **Балансировка нагрузки**: трафик распределяется между несколькими каналами, что предотвращает перегрузку отдельных линий.
4. **Экономия ресурсов**: нет необходимости заменять существующее оборудование для увеличения пропускной способности.

Рассмотрим сеть на рисунке 1.

Рисунок 1 – Пример топологии

В данной топологии порты между коммутаторами не агрегированы, между ними есть только два параллельных физических канала связи. В результате, в сети возникает петля, которую «разрывает» протокол STP (Spanning Tree Protocol). Таким образом, добавление соединения между коммутаторами ничего не меняет, так как данные по-прежнему передаются только через один канал. Единственное преимущество — появление резервного канала для передачи данных, который включится при разрыве активного соединения.

Чтобы порты обменивались данными одновременно, необходимо настроить агрегацию. Это можно сделать либо вручную, либо используя протоколы.

EtherChannel – это технология, которая позволяет агрегировать несколько физических каналов в единый логический интерфейс. Термин etherchannel введён компанией Cisco, другие вендоры могут называть агрегирование по-своему (например, Link Aggregation Group (LAG) или Port Channel).

Для реализации агрегации каналов используются специальные протоколы, обеспечивающие согласованную работу устройств. Наиболее распространёнными протоколами являются LACP и PAgP.

Протокол LACP (Link Aggregation Control Protocol) описан в стандарте IEEE 802.3ad. Данный протокол поддерживает два режима: active и passive. Режим active сразу включает протокол LACP, а режим passive включит LACP только если обнаружит LACP-сообщение от соседа. Таким образом, чтобы объединить порты с использованием протокола LACP, необходимо перевести протокол в режим active хотя бы на одном из двух устройств.

PAgP (Port Aggregation Protocol) – проприетарный протокол, разработанный компанией Cisco. Данный протокол не поддерживает мультивендорную среду, так как работает только на оборудовании Cisco. Большинство сетей строятся на оборудовании разных вендоров, поэтому PAgP используется достаточно редко.

Поддерживает режимы auto и desirable. Для успешной агрегации необходимо переключить протокол в режим desirable хотя бы на одном устройстве.

Вне зависимости от используемого протокола агрегации, настраиваемые порты должны быть идентичны друг другу, т.е. иметь одинаковую скорость, разрешенные vlan-ы и одинаковый режим (access/trunk).

Рассмотрим подробнее процесс агрегации на примере протокола LACP.

Протокол LACP использует сообщения LACPDU (Link Aggregation Control Protocol Data Units) для обмена информацией с соседней стороной. После переключения протокола в режим active, порт посылает LACPDU, чтобы передать соседней стороне свои параметры. LACPDU содержит следующие данные:

System Priority: Приоритет устройства (0–65535). Чем меньше значение, тем выше приоритет.

System ID: MAC-адрес коммутатора. Если System Priority совпадает, сравниваются System ID (MAC-адреса). Устройство с меньшим MAC-адресом становится управляющим.

Port Priority: Приоритет порта (0–255).

Port Number: Идентификатор порта.

Key: Ключ агрегации. Порты с одинаковым ключом могут быть объединены.

State: Состояние порта (активен, готов к агрегации и т.д.).

Когда коммутатор получает LACPDU, он сравнивает полученные параметры, с информацией о своих портах, настроенных на агрегацию. Если параметры совпадают, порты объединяются в агрегированный канал. Количество физических портов, которые можно объединить в один логический, ограничено. Как правило, объединить можно не более 8 портов. Если портов больше, в агрегированный канал подключаются порты с наименьшими Port Priority и Port Number. Остальные порты становятся резервными.

Резервирование.

В сетях с критически важными сервисами обеспечение отказоустойчивости шлюзов по умолчанию является обязательным требованием. Если шлюз выходит из строя, а резервирование отсутствует, все устройства, зависящие от этого шлюза, теряют возможность взаимодействовать с другими сегментами сети или внешними ресурсами. Это приводит к полному прекращению передачи данных через данный

узел: внутренние сервисы становятся недоступными, пользователи не могут получить доступ к интернету или корпоративным системам, а любые операции, требующие маршрутизации, останавливаются. Восстановление работы в таких случаях требует ручного вмешательства, что увеличивает время простоя. Резервирование шлюзов позволяет избежать этих проблем, обеспечивая автоматическое и мгновенное переключение передачи трафика на резервный узел без существенных задержек. Рисунок 2 наглядно демонстрирует принцип резервирования шлюзов.

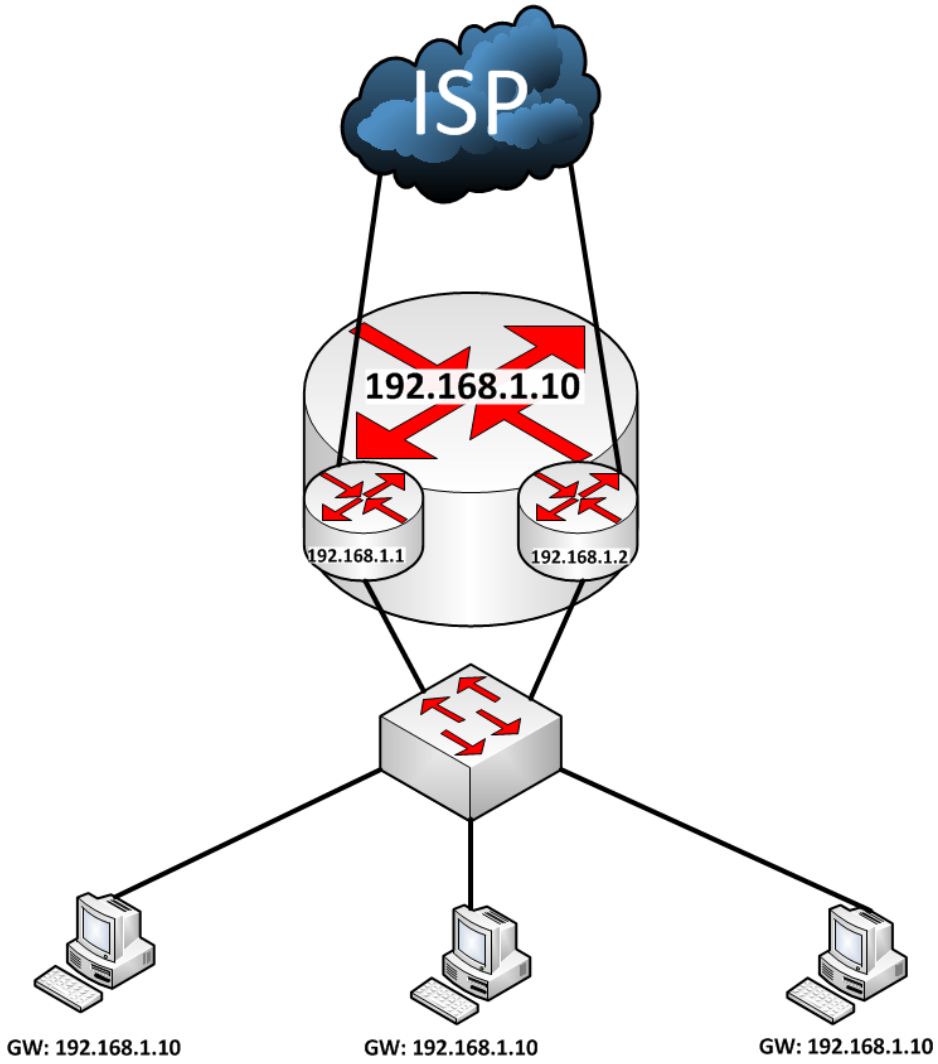

Рисунок 2 – Резервирование шлюзов

В данной сети два маршрутизатора объединены в виртуальный маршрутизатор с адресом 192.168.1.10, который используется клиентами в качестве шлюза по умолчанию. В процессе передачи данных клиентов может быть выбран

как один маршрутизатор группы, так и несколько, в зависимости от используемого протокола резервирования и балансировки нагрузки.

Для обеспечения отказоустойчивости сетевой инфраструктуры используются протоколы семейства FHRP (First Hop Redundancy Protocol). Они позволяют создать группу маршрутизаторов, один из которых выполняет роль активного шлюза, а остальные – резервных, готовых моментально принять управление в случае сбоя основного устройства. Использование неизменных виртуальных IP и MAC адресов обеспечивает для конечных пользователей неизменность настроек.

К основным протоколам группы FHRP относятся HSRP, VRRP и GLBP.

HSRP (Hot Standby Router Protocol)

Проприетарный протокол Cisco, который обеспечивает резервирование шлюзов в локальных сетях.

Принцип работы протокола следующий:

1. Группа маршрутизаторов объединяется в HSRP-группу.
2. Один маршрутизатор становится Active (активным), остальные — Standby(резервными).
3. Все устройства в группе используют виртуальный IP-адрес и виртуальный MAC-адрес, который предоставляется клиентам в качестве шлюза по умолчанию.
4. Активный маршрутизатор обрабатывает весь трафик. В случае его сбоя резервный маршрутизатор мгновенно берет на себя роль активного.

Каждое устройство имеет свой приоритет (0-255) устройство с наивысшим приоритетом становится активным. По умолчанию приоритет HSRP равен 100. Если приоритет не определён то, используется это значение. Если ни одному из маршрутизаторов в группе не был назначен приоритет, то приоритеты всех маршрутизаторов совпадут и активным в этом случае станет маршрутизатор с наибольшим IP-адресом интерфейса, на котором настроен HSRP.

Режим preempt позволяет маршрутизатору с более высоким приоритетом перехватывать роль active маршрутизатора. По умолчанию, режим preempt выключен.

Устройства обмениваются служебными сообщениями каждые 3 секунды. Если активный маршрутизатор не посылает сообщения в течении 10 секунд, то

происходит переключение. Эти таймеры настраиваются, их значения могут быть от 1 до 255 секунд. Значения таймеров для всех маршрутизаторов одной группы HSRP должны быть одинаковыми.

VRRP (Virtual Router Redundancy Protocol)

Протокол VRRP это открытый стандарт резервирования шлюзов, описанный в RFC 5798. В отличие от проприетарного протокола, HSRP, VRRP поддерживается оборудованием разных вендоров, что делает его универсальным решением.

Группа маршрутизаторов образует VRRP-группу (объединяются в один виртуальный маршрутизатор). Все маршрутизаторы в группе имеют общий виртуальный IP (VIP) адрес и общий номер группы или VRID (Virtual Router Identifier). Один маршрутизатор может состоять в нескольких группах, каждая из которых должна иметь свою уникальную пару VIP/VRID.

Все маршрутизаторы делятся на два типа: VRRP Master и VRRP Backup. VRRP Master передаёт пакеты, а VRRP Backup выполняют роль резервных маршрутизаторов.

Выбор Master маршрутизатора, как и active маршрутизатора в протоколе HSRP, осуществляется на основе приоритетов и IP адресов. Устройства могут иметь приоритет в диапазоне от 1 до 254. Маршрутизатор с наивысшим приоритетом становится Master. В случае совпадения приоритетов, главным становится маршрутизатор с наибольшим IP адресом. Маршрутизатор, имеющий IP адрес, совпадающий с виртуальным IP адресом группы, становится главным (его приоритет автоматически становится равным 255). Аналогично HSRP, в протоколе VRRP есть возможность настройки режима preempt. Если этот режим включён, Backup маршрутизатор может изменить роль на Master, имея наивысший приоритет. По умолчанию режим preempt отключен.

Приведённые выше протоколы позволяют задействовать только один маршрутизатор для передачи трафика, что обеспечивает надёжность, но не решает проблему неэффективного использования сетевых ресурсов. Резервные маршрутизаторы в этих протоколах остаются пассивными до момента сбоя, что приводит к избыточности мощностей. Балансировка нагрузки становится ключевым элементом в преодолении этих ограничений. Она не только гарантирует

непрерывность работы при отказах, но и позволяет распределять трафик между несколькими узлами, предотвращая перегрузку отдельных устройств.

GLBP (Gateway Load Balancing Protocol)

GLBP (Gateway Load Balancing Protocol) — ещё один протокол группы FHRP. Как и HSRP, данный протокол проприетарный, принадлежит компании Cisco и работает только на устройствах этого вендора. Отличительной особенностью протокола GLBP является поддержка балансировки нагрузки между несколькими маршрутизаторами. Таким образом, данный протокол не только обеспечивает отказоустойчивость, но и оптимизирует использование сетевых ресурсов, распределяя трафик между маршрутизаторами, объединёнными в группу.

Принцип работы:

Маршрутизаторы объединяются в группу с общим виртуальным IP-адресом, который используется клиентами как адрес шлюза по умолчанию.

Каждый маршрутизатор получает виртуальный MAC-адрес, который используется для обработки трафика клиентов, направляемого на него через ARP-запросы от Active Virtual Gateway (AVG). Эти виртуальные MAC-адреса позволяют распределить нагрузку между несколькими маршрутизаторами в группе GLBP, обеспечивая балансировку и отказоустойчивость.

Маршрутизаторы, объединённые в группу GLBP, могут иметь две роли: Active Virtual Gateway (AVG) и Active Virtual Forwarder (AVF). AVG – это главный маршрутизатор, управляющий распределением виртуальных MAC-адресов между участниками группы. Этот маршрутизатор отвечает за ответы на ARP-запросы клиентов, направляя их к разным маршрутизаторам. AVF маршрутизаторы обрабатывают трафик клиентов. Каждый маршрутизатор имеет приоритет (1-255). В случае выхода AVG из строя, его роль переходит к маршрутизатору с наивысшим приоритетом.

Протокол GLBP поддерживает несколько режимов распределения трафика:

Round Robin – маршрутизатор AVG выдаёт клиентам MAC-адреса AVF попеременно, что обеспечивает равномерное распределение нагрузки между всеми активными маршрутизаторами в группе GLBP. Каждый новый ARP-запрос от

клиента получает следующий виртуальный MAC-адрес из списка доступных AVF. Этот режим балансировки используется протоколом GLBP по умолчанию.

Host-Dependent позволяет закрепить за клиентом один маршрутизатор. На ARP-запросы клиента всегда будет возвращаться один MAC-адрес.

Weighted – режим, при котором балансировка нагрузки производится в соответствии с весовым коэффициентом каждого устройства. Это значение задаётся вручную на каждом устройстве. Таким образом, маршрутизаторы, имеющие большую пропускную способность, могут принимать на себя больше трафика.

None – балансировка нагрузки не обеспечивается. Все запросы клиентов выполняются AVG. Другой маршрутизатор будет задействован только в том случае, если AVG выйдет из строя.

Маршрутизаторы в группе обмениваются Hello-пакетами для поддержания актуальной информации о состоянии устройств в группе. По умолчанию, рассылка осуществляется каждые 3 секунды. Возможность включение режима preempt также предусмотрена.

В одной группе GLBP может быть не более 4 маршрутизаторов. Если в группу добавлено больше четырёх устройств, только первые четыре маршрутизатора будут активно участвовать в обработке трафика, а остальные перейдут в состояние резерва. Эти резервные маршрутизаторы будут ожидать, пока один из активных участников группы выйдет из строя, чтобы занять его место и начать обработку трафика.

Сочетание агрегации каналов, резервирования и балансировки нагрузки позволяет создать сеть, которая не только устойчива к сбоям, но и эффективно использует ресурсы. Выбор конкретных технологий (LACP/PAgP, HSRP/VRRP/GLBP) зависит от требований к мультивендорности, уровню автоматизации и необходимости балансировки. В условиях растущих нагрузок и требований к доступности, интеграция этих решений становится не просто рекомендацией, а необходимостью.

Контрольные вопросы:

1. С какой целью устанавливается пара идентификаторов VIP/VRID?
2. Назовите основные отличия протоколов LACP и PAgP

3. Какие ограничения существуют в технологиях агрегирования каналов? (ответ может зависеть от вендора, предлагается рассмотреть ограничения Cisco)
4. Какая технология балансировки трафика наиболее применима к современным компьютерным сетям и почему?