

Лабораторная работа: изучение технологии SLB

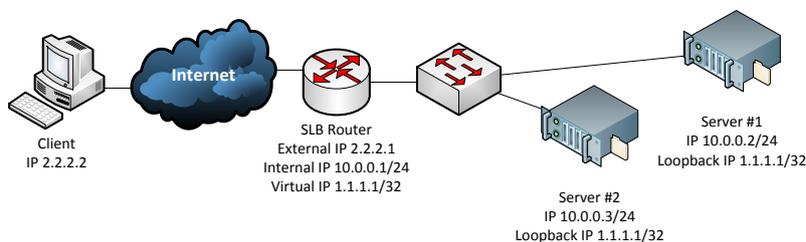
Введение

Технология Cisco SLB (Server Load Balancing) предназначена для распределения нагрузки между несколькими серверами, а также для обеспечения отказоустойчивости предоставляемого сервиса, так как обеспечивает продолжение функционирования последнего даже при отказе одного или нескольких серверов. SLB – не единственная технология, с помощью которой возможно распределение нагрузки, часто в реальных сетях также применяют NLB или балансировку с помощью DNS. Возможно даже совмещение нескольких вариантов распределения нагрузки и использование специализированных балансировщиков.

Cisco Server Load Balancing может работать в двух режимах: L2 и L3. Наиболее простым для понимания и реализации является L3 режим, в котором маршрутизатор выполняет не только распределение TCP или UDP сессий между серверами, но и изменение IP-адреса получателя (NAT) иногда вместе с TCP/UDP портом получателя (PAT). В качестве адреса получателя выбирается реальный адрес сервера. Преимуществом данного метода балансировки является возможность нахождения балансирующего маршрутизатора и серверов в разных L3 сетях. К недостаткам можно отнести повышенную нагрузку на процессор, обусловленную выполнением NAT/PAT.

При работе в L2 режиме трансляция NAT/PAT не выполняется, то есть адрес получателя и порт остаются неизменными. «Выбор» сервера осуществляется лишь на основе изменения MAC-адреса получателя. Таким образом, к серверам применяется дополнительное требование: операционная система должна иметь постоянно работающий интерфейс, на котором назначен IP-адрес сервиса. Назначение такого IP-адреса непосредственно на Ethernet-интерфейс (вторичный (secondary) адрес) не является хорошей идеей, так как при переходе его в рабочее состояние будет произведён широковещательный ARP-запрос об этом адресе, что приведёт к появлению сообщения об ошибке дублирования IP-адресов в сети (ответят другие аналогичные сервера). На практике для указанной цели используют специальные интерфейсы замыкания на себя (Loopback).

Пример сети, в которой работает SLB, представлен ниже. Стоит отметить, что интерфейсы Loopback на серверах в этой схеме будут использоваться только в случае использования L2 режима SLB. Маски для клиента и внешнего интерфейса маршрутизатора не указаны, так как в реальной сети эти адреса, конечно же, будут из разных подсетей и могут быть произвольными.



Практическое задание

Конфигурирование устройств в данной лабораторной работе делится на три части: сначала собирается схема для режима L3, после чего производится перенастройка для перехода на L2, далее (только при работе в эмуляторе) производится построение отказоустойчивой схемы балансировки. Отдельно стоит отметить, что данную лабораторную работу стоит выполнять лишь после того, как хорошо освоены предыдущие (более простые) работы. Здесь нет чёткой последовательности действий для всех пунктов настройки, что оставляет простор для творчества у студента, позволяя наиболее полно ознакомиться со всеми вспомогательными опциями. Часть №3 выполняется только на эмуляторе.

При выполнении данной лабораторной работы на реальном оборудовании в качестве маршрутизатора с SLB используйте Cisco 3640, при работе на эмуляторе выбирайте маршрутизатор Cisco серии 7200. Также при работе в эмуляторе в качестве клиента и серверов можно использовать маршрутизаторы.

Часть №1

1. Выполните все необходимые соединения и произведите все необходимые подготовительные настройки (назначение IP-адресов, настройка маршрутизации, конфигурирование виртуальных сетей на коммутаторе). Убедитесь в работоспособности полученной схемы. Следует понимать, что в реальной сети доступа к серверам извне не будет по двум причинам: во-первых, приватные IP-адреса не маршрутизируются глобально, а во-вторых, все «лишние» доступы закрываются с помощью списков доступа.

2. На SLB маршрутизаторе из режима глобальной конфигурации перейдите в режим настройки виртуальной фермы серверов *test* с помощью команды **ip slb serverfarm test**.
3. Дайте команду **nat server** для перевода фермы в режим работы L3.
4. Определитесь, какой сервис будет запущен для тестирования собираемой схемы. При работе в эмуляторе в качестве сервиса можно использовать telnet к «маршрутизаторам-серверам». С помощью команды **real 10.0.0.2 port** перейдите в режим настройки сервера 10.0.0.2 внутри данной фермы, где *port* – номер порта, на котором работает тестируемый сервис. Командой **inservice** переведите данный сервер внутри фермы в рабочее состояние. Повторите указанную процедуру для второго сервера. В общем случае номер порта конкретного сервера может отличаться от номеров портов других серверов и внешнего порта сервиса в целом.
5. Изучите следующие вспомогательные опции: **faildetect**, **maxconns**, **predictor**, **retry** и **weight**.
6. С помощью команд привилегированного режима **sho ip slb serverfarms**, **sho ip slb serverfarms detail**, **sho ip slb reals** изучите статусы серверных ферм и включённых в их состав серверов.
7. Используйте команду **ip slb vserver test** для перехода в режим настройки виртуального сервера *test*.
8. С помощью команды **serverfarm test** привяжите ранее созданную серверную ферму *test* к данному виртуальному серверу.
9. Указать адрес (в данной работе это 1.1.1.1), протокол и порт внешнего сервиса можно с помощью команды **virtual 1.1.1.1 protocol port**.
10. Переведите виртуальный сервер в рабочий режим с помощью команды **inservice**. Дополнительно изучите возможности следующих опций: **advertise**, **client**, **sticky** и **synguard**.
11. Изучите возможности просмотрных команд **sho ip slb conns**, **sho ip slb reals**, **sho ip slb stats**, **sho ip slb sticky**, **sho ip slb vservers** и **sho ip slb wildcard**.
12. Запустите тестовые сервисы на тестовых серверах и произведите подключение клиентом. На реальном оборудовании с помощью утилит netcps, iperf или аналогичных измерьте производительность маршрутизатора с SLB в режиме L3.
13. Убедитесь в том, что отключение любого из серверов не приводит к падению сервиса.

Часть №2

1. На тестовых серверах (или маршрутизаторах при работе в эмуляторе) создайте интерфейс Loopback, на который назначьте адрес 1.1.1.1.
2. Создайте новую серверную ферму, однако в ней не давайте команду **nat server**.
3. Добавьте сервера в новую ферму. При добавлении сервера в L2 ферму не нужно указывать порт.
4. Переведите виртуальный сервер *test* в нерабочий режим.
5. Замените ферму в виртуальном сервере *test* на новую.
6. Переведите виртуальный сервер *test* в рабочий режим.
7. Убедитесь в работоспособности нового режима работы SLB.
8. Проверьте доступность сервиса при отключении любого из серверов.

Часть №3

1. Соберите новую схему так, чтобы параллельно с маршрутизатором SLB был установлен новый маршрутизатор той же модели с той же версией IOS.
2. На старом и новом маршрутизаторах настройте HSRP с именованной группой.
3. Переведите виртуальный сервер *test* в нерабочий режим.
4. Скопируйте настройки со старого маршрутизатора SLB на новый.
5. На обоих маршрутизаторах переведите виртуальный сервер *test* в рабочий режим с помощью команды **inservice standby name**, где *name* – имя сконфигурированной ранее группы HSRP.
6. Убедитесь, что статус виртуального сервера зависит от статуса узла в настроенной HSRP-группе.
7. Проверьте отказоустойчивость новой схемы путём попеременного отключения маршрутизаторов SLB.