Применение технологии IP SLA для обеспечения отказоустойчивости сети

Н. П. Кураков, email: kalkree@gmail.com[1]
М. К. Чернышов, email: mkch69@gmail.com [1]

[1] Воронежский государственный университет

Аннотация. *В работе рассматривается один из методов обеспечения отказоустойчивости сети, реализуемый с помощью технологии IP SLA на сетевом уровне модели OSI в сетевой лаборатории EVE-NG с использованием маршрутизаторов Cisco и Mikrotik, обеспечивающий дублирование ключевого соединения между маршрутизаторами.*

Ключевые слова: *Глобальные сети, маршрутизация, отказоустойчивость сети, ключевое соединение, промежуточная сеть.*

Введение

Большинство современных компьютеров образует между собой компьютерные сети, будь то крупное предприятие или локальная домашняя сеть. Как правило, при конфигурировании и настройке сети необходимо обеспечивать доступ к тем или иным ключевым узлам сети, серверам, Интернету. При этом в компьютерных сетях, как и везде, случаются сбои, оказывающие влияние на работоспособность системы в целом. В итоге все чаще возникает вопрос о том, каким образом решать проблему отказоустойчивости в компьютерных сетях.

Как известно, отказоустойчивость сети характеризуется двумя параметрами: избыточностью (количеством дублированных соединений) и временем восстановления после сбоя. С физической, аппаратной точки зрения решение всегда одно – дублирование ключевого соединения. Однако, при использовании программного, логического подхода к изучению данной проблемы можно говорить о множестве различных способов ее решения. Большинство из них реализуется на канальном и сетевом уровнях сетевой модели OSI. В данной работе рассматривается один из современных методов обеспечения отказоустойчивости компьютерной сети, основанный на использовании технологии IP SLA [1], работающий на сетевом уровне модели OSI.

Помимо технологии IP SLA существует много аналогов, имеющие свои преимущества и недостатки, однако, в отношении их данная

технология является наиболее предпочтительной по причине отсутствия требований серьёзных возможностей от аппаратуры, минимальной нагрузки на сеть и быстрого восстановления работоспособности.

1. Схема сети. Постановка задачи

На рисунке представлена схема локальной сети с дублированием ключевого соединения между двумя маршрутизаторами. Схема построена и реализована в рамках сетевой лаборатории EVE-NG [2].

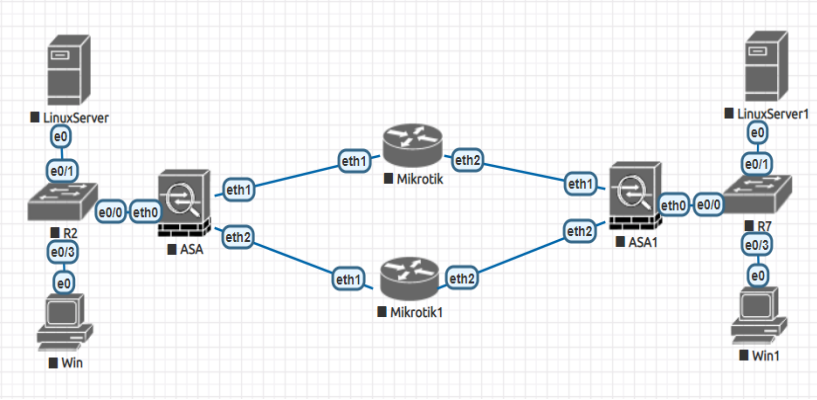

Рисунок. Примерная схема локальной сети

Рассмотрим структуру данной сети подробнее. Присутствуют две локальные сети с маршрутизаторами Cisco серии ASA (ASA и ASA1) и между ними два роутера Mikrotik, эмулирующие промежуточные сети (Miktotik и Mikrotik1). Считается, что соединение через «верхнюю» промежуточную сеть (Mikrotik) является основным, а через «нижнюю» – резервным. В случае штатной работы должен использоваться основной маршрут, в случае его отказа должен быть осуществлён переход на резервный.

В каждой локальной сети присутствуют рабочие станции под управлением ОС Windows и ОС Linux. Рабочие станции Windows использовались для настройки маршрутизаторов, а Linux – для тестирования работы полученной системы. Для удобства в каждой локальной сети был установлен и запущен локальный веб-сервер nginx с изменённой стартовой страницей для определения сервера, к которому выполнено подключение.

Рабочие станции под управлением ОС Windows получают IP адрес по DHCP, ОС Linux имеет статический адрес. А каждый маршрутизатор

транслирует трафик с «уличного», внешнего интерфейса, на адрес рабочей станции с установленным nginx.

В данной работе промежуточные узлы должны только пропускать трафик между интерфейсами. В реальной системе в этом месте может быть представлена другая локальная сеть со своим маршрутизатором, который отслеживает и анализирует получаемые пакеты.

2. Этапы реализации отказоустойчивости

Алгоритм решения поставленной задачи состоит из нескольких шагов.

Вначале требуется произвести базовую настройку маршрутизаторов конечных сетей, а именно настроить активные интерфейсы – указать их адреса и маски, настроить работу по протоколу DHCP.

```
interface Ethernet0
 nameif inside
 security-level 100
 ip address 192.168.50.1 255.255.255.0
!
interface Ethernet1
 nameif tomiddlenet1
 security-level 0
 ip address 192.168.101.10 255.255.255.0
!
interface Ethernet2
 nameif tomiddlenet2
 security-level 0
 ip address 192.168.102.10 255.255.255.0
!
dhcpd address 192.168.50.10-192.168.50.50 inside
dhcpd enable inside
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
http 192.168.50.0 255.255.255.0 inside
ssh 192.168.50.0 255.255.255.0 inside
crypto key generate rsa
username asdmadmin password asdmadmin privilege 15
```

Далее необходимо настроить службу IP SLA и функционирование механизма переключения track. Для этого нужно включить службу sla monitor и указать необходимые параметры (число пакетов, необходимых для объявления узла недоступным; частоту отправки ICMP пакетов; «график» и время работы службы и т.д.). После чего уже подключить её к механизму track, который будет отслеживать состояние sla monitor и в

зависимости от состояния службы выключать или выключать основной маршрут.

```
sla monitor 123
type echo protocol ipIcmpEcho 192.168.101.200 interface
tomiddlenet1
 num-packets 3
 frequency 5
sla monitor schedule 123 life forever start-time now
!
track 1 rtr 123 reachability
```

Следующим шагом является установка путей на маршрутизаторах конечных сетей. Как было сказано ранее, «верхний» маршрут является основным, соответственно он будет иметь наивысший приоритет, но к нему необходимо подключить сконфигурированный ранее механизм track. Резервный маршрут имеет меньший приоритет и работает всегда, вне зависимости от состояния track.

```
route tomiddlenet1 0.0.0.0 0.0.0.0 192.168.101.200 1 track 1
route tomiddlenet2 0.0.0.0 0.0.0.0 192.168.102.200 254
```

Последним шагом в конфигурации маршрутизаторов является настройка NAT для трансляции входного трафика на локальный веб-сервер. В данной работе достаточно получать только пакеты по 80 и 8080 порту, поскольку nginx в базовой конфигурации использует только их.

```
access-list input1 extended permit tcp any object server1 eq
www
access-list input1 extended permit tcp any object server1 eq
8080
access-list input2 extended permit tcp any object server2 eq
www
access-list input2 extended permit tcp any object server2 eq
8080
access-group input1 in interface tomiddlenet1
access-group input2 in interface tomiddlenet2
object network server1
 nat (inside,tomiddlenet1) static interface
object network server2
 nat (inside,tomiddlenet2) static interface
```

В данной работе промежуточные сети используются только в качестве посредников, соответственно, достаточно настроить сетевой мост между интерфейсами, чтобы они находились в одной локальной сети и могли транслировать трафик между собой.

```
/interface ethernet set [find default-name=ether1]
name=middlenet1
/interface ethernet set [find default-name=ether2]
name=middlenet2
/interface bridge add name=middlenet
/interface bridge port add interface=middlenet1
bridge=middlenet
/interface bridge port add interface=middlenet2
bridge=middlenet
ip address add address=192.168.101.200/255.255.255.0
interface=middlenet
```

В итоге, в случае штатной работы системы трафик будет идти через основной маршрут, но если в процессе работы выключить узел Mikrotik, то после получения таймаутов по 3 отправленным ICMP пакетам автоматически будет осуществлен переход на резервный маршрут.

Заключение

Таким образом, благодаря использованию технологии IP SLA была решена проблема отказоустойчивости сети без серьёзного повышения нагрузки на сетевое оборудование и с достаточно быстрым восстановлением соединения.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 19-07-00037.

Список литературы

1. IP SLA [Электронный ресурс] : статья. – Режим доступа : http://ciscomaster.ru/node/9/

2. Сетевая лаборатория EVE-NG [Электронный ресурс] : статья. – Режим доступа : https://www.eve-ng.net/