Лабораторная работа № 9. Использование протокола STP. Агрегирование каналов

9.1. Цель работы

Изучение возможностей протокола STP и его модификаций по обеспечению отказоустойчивости сети, агрегированию интерфейсов и перераспределению нагрузки между ними.

9.2. Предварительные сведения

9.2.1. Протокол STP

Основное назначение протокола STP (Spanning Tree Protocol, протокол остовного дерева) — устранение петель в топологии сети на базе технологии Ethernet при наличии избыточных соединений.

Протокол STP функционирует на канальном уровне модели OSI, его описание приведено в стандарте IEEE 802.1d [1]. В основе работы протокола лежит одноимённый алгоритм — Spanning Tree Algorithm (STA, алгоритм остовного дерева).

Принцип работы протокола STP заключается в следующем:

- одно из коммутационных устройств сети, являющееся частью топологии сети с избыточными соединениями, выбирается в качестве корневого устройства (Root Bridge);
- на основе алгоритма остовного дерева остальные коммутаторы сети определяют для себя так называемые «корневые порты» (Root Port) — порты, считающиеся по определённой метрике ближайшими относительно корневого устройства;
- остальные сетевые порты, имеющие соединение с корневым устройством, блокируются.

9.2.2. Bridge Protocol Data Unit

Во время функционирования протокола STP устройства сети обмениваются сообщения BPDU (Bridge Protocol Data Unit), определёнными в стандарте IEEE 802.1d.

BPDU содержит следующие поля:

- идентификатор версии протокола STP (Protocol Identifier, 2 байта);
- номер версии протокола STP (Version, 1 байт);
- тип BPDU (Message Type, 1 байт) — конфигурационный (Configuration BPDU) или уведомляющий об изменении топологии (Topology Change Notification BPDU);
- флаги (Flags, 1 байт):
  - TC (Topology Change) — 1-й по порядку бит в поле флагов — указание на изменение топологии;
  - TCA (Topology Change Acknowledgment) — 8-й по порядку бит в поле флагов — подтверждение получения пакета BPDU с установленным битом TC;
- идентификатор корневого устройства (Root Bridge ID или Root ID, 8 байт);

– расстояние до корневого устройства (Root Path Cost, 4 байта);
– идентификатор отправителя (Bridge ID или Switch ID, 8 байт);
– идентификатор порта (Port ID, 2 байта);
– время жизни сообщения (Message Age, 2 байта);
– максимальное время жизни сообщения (Maximum Age, 2 байта);
– интервал hello (Hello Time, 2 байта) — интервал, через который посылаются пакеты BPDU;
– задержка смены состояний (Forward Delay, 2 байта) — минимальное время перехода коммутатора из активного в пассивное состояние, и наоборот.

9.2.3. Типы состояний портов, работающих по протоколу STP

Определены 4 типа состояний портов, работающих по протоколу STP:
– порт блокирован (Blocking State) — порт не участвует в обмене сообщениями;
– порт в состоянии прослушивания (Listening State) — осуществляется приём BPDU, но не происходит определения места назначения, операций фильтрации и передачи пользовательской информации; возможен переход порта в состояние блокировки или обучения;
– порт в состоянии обучения (Learning State) — состояние, предшествующее переходу в состояние передачи (при этом запоминается расположение ближайших устройств и обновление адресной таблицы);
– порт в состоянии передачи (Forwarding State) — порт участвует в обмене сообщениями, определении расположения станций в сети, фильтрации данных и передаче пользовательского трафика.

9.2.4. Модификации STP

Протокол Rapid Spanning Tree Protocol (RSTP) описан в документах IEEE 802.1w-2001 и IEEE 802.1D-2004. По сравнению с STP реализует ускоренную реконфигурацию дерева для исключения петель, т.е. уменьшилось время построения топологии, а также время восстановления работоспособности сети при смене маршрута следования пакетов. Порт может находиться в одном из трёх состояний: Discarding, Learning, Forwarding.

Per-VLAN Spanning Tree Protocol (PVSTP) — проприетарное расширение протокола STP, разработанное компанией Cisco. Позволяет использовать отдельные настройки (экземпляры) протокола STP для разных VLAN. Работает только при использовании портов в режиме ISL-транк (проприетарный протокол компании Cisco для передачи информации о принадлежности трафика к определённому VLAN).

PVSTP+ — модификация PVSTP, работающая при использовании портов в режиме 802.1Q-транк (тегирование трафика для передачи информации о принадлежности к VLAN).

Rapid PVST+ — модификация, объединяющая свойства PVST+ и RSTP за счёт использования мультикастовых фреймов.

Multiple Spanning Tree Protocol (MSTP) — используется один экземпляр протокола для нескольких VLAN при условии идентичности их топологий. Протокол MSTP описан в документах IEEE 802.1s и 802.1Q-2003.

9.3. Задание

1. Сформируйте резервное соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-3`.
2. Настройте балансировку нагрузки между резервными соединениями.
3. Настройте режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы.
4. Изучите отказоустойчивость резервного соединения.
5. Сформируйте и настройте агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-4`.
6. При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

9.4. Последовательность выполнения работы

1. Сформируйте резервное соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-3` (рис. 9.1). Для этого:
   - замените соединение между коммутаторами `msk-donskaya-sw-1` (Gig0/2) и `msk-donskaya-sw-4` (Gig0/1) на соединение между коммутаторами `msk-donskaya-sw-1` (Gig0/2) и `msk-donskaya-sw-3` (Gig0/2);
   - сделайте порт на интерфейсе Gig0/2 коммутатора `msk-donskaya-sw-3` транковым:

     ```
     msk-donskaya-sw-3(config)#int g0/2
     msk-donskaya-sw-3(config-if)#switchport mode trunk
     ```

   - соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-4` сделайте через интерфейсы Fa0/23, не забыв активировать их в транковом режиме.

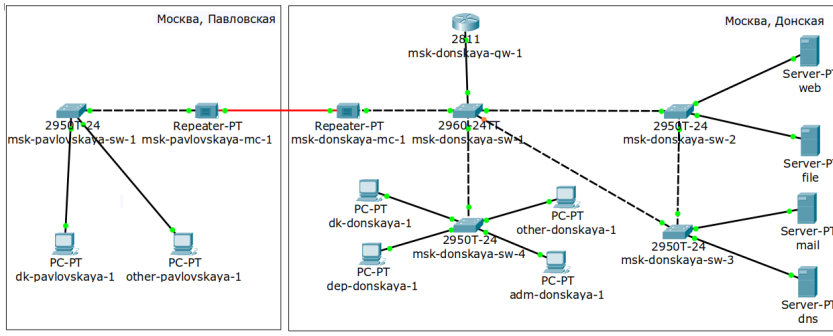

Рис. 9.1. Логическая схема локальной сети с резервным соединением

2. С оконечного устройства `dk-donskaya-1` пропингуйте серверы `mail` и `web`. В режиме симуляции проследите движение пакетов ICMP. Убедитесь, что движение пакетов происходит через коммутатор `msk-donskaya-sw-2`.

3. На коммутаторе `msk-donskaya-sw-2` посмотрите состояние протокола STP для vlan 3:

```
msk-donskaya-sw-2#show spanning-tree vlan 3
```

В результате будет выведена примерно следующая информация, связанная с протоколом STP:

```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    32771
             Address     0001.9698.29B8
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     0001.9698.29B8
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Здесь, в частности, указывается, что данное устройство является корневым (строка `This bridge is the root`).

4. В качестве корневого коммутатора STP настройте коммутатор `msk-donskaya-sw-1`:

```
msk-donskaya-sw-1#configure terminal
msk-donskaya-sw-1(config)#spanning-tree vlan 3 root primary
```

5. Используя режим симуляции, убедитесь, что пакеты ICMP пойдут от хоста `dk-donskaya-1` до `mail` через коммутаторы `msk-donskaya-sw-1` и `msk-donskaya-sw-3`, а от хоста `dk-donskaya-1` до `web` через коммутаторы `msk-donskaya-sw-1` и `msk-donskaya-sw-2`.
6. Настройте режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы:

```
msk-donskaya-sw-2(config)#interface f0/1
msk-donskaya-sw-2(config-if)#spanning-tree portfast

msk-donskaya-sw-2(config)#interface f0/2
msk-donskaya-sw-2(config-if)#spanning-tree portfast


msk-donskaya-sw-3(config)#interface f0/1
msk-donskaya-sw-3(config-if)#spanning-tree portfast

msk-donskaya-sw-3(config)#interface f0/2
msk-donskaya-sw-3(config-if)#spanning-tree portfast
```

7. Изучите отказоустойчивость протокола STP и время восстановления соединения при переключении на резервное соединение. Для этого используйте команду `ping -n 1000 mail.donskaya.rudn.ru` на хосте `dk-donskaya-1`, а разрыв соединения обеспечьте переводом соответствующего интерфейса коммутатора в состояние `shutdown`.

8. Переключите коммутаторы режим работы по протоколу Rapid PVST+:

```
msk-donskaya-sw-1(config)#spanning-tree mode rapid-pvst
msk-donskaya-sw-2(config)#spanning-tree mode rapid-pvst
msk-donskaya-sw-3(config)#spanning-tree mode rapid-pvst
msk-donskaya-sw-4(config)#spanning-tree mode rapid-pvst
msk-pavlovskaya-sw-1(config)#spanning-tree mode rapid-pvst
```

9. Изучите отказоустойчивость протокола Rapid PVST+ и время восстановления соединения при переключении на резервное соединение.
10. Сформируйте агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-4` (рис. 9.2).

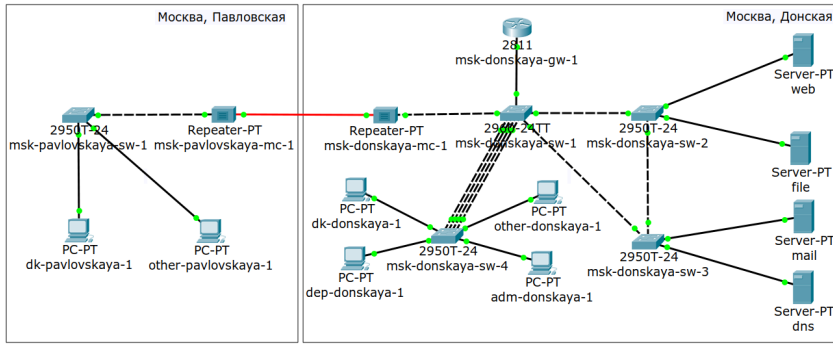

Рис. 9.2. Логическая схема локальной сети с агрегированным соединением

11. Настройте агрегирование каналов (режим EtherChannel):

```
msk-donskaya-sw-1(config)#interface range f0/20 - 23
msk-donskaya-sw-1(config-if-range)#channel-group 1 mode on
msk-donskaya-sw-1(config-if-range)#exit
msk-donskaya-sw-1(config)#interface port-channel 1
msk-donskaya-sw-1(config-if)#switchport mode trunk

msk-donskaya-sw-4(config)#int range f0/20 - 23
msk-donskaya-sw-4(config-if-range)#no switchport access vlan 104
msk-donskaya-sw-4(config-if-range)#exit

msk-donskaya-sw-4(config)#interface range f0/20 - 23
msk-donskaya-sw-4(config-if-range)#channel-group 1 mode on
msk-donskaya-sw-4(config-if-range)#exit
msk-donskaya-sw-4(config)#interface port-channel 1
msk-donskaya-sw-4(config-if)#switchport mode trunk
```

Здесь использована следующая терминология Cisco:

- `EtherChannel` — технология агрегирования каналов;
- `port-channel` — логический интерфейс, который объединяет физические интерфейсы;
- `channel-group` — команда, которая указывает, какому логическому интерфейсу принадлежит физический интерфейс и какой режим используется для агрегирования;

  - возможные параметры `channel-group`:
    - `active` — включить LACP;
    - `passive` — включить LACP, только если придёт сообщение LACP;
    - `desirable` — включить PAgP;
    - `auto` — включить PAgP, только если придёт сообщение PAgP;
    - `on` — включить только EtherChannel.

9.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - подробное описание настроек сетевого оборудования в соответствии с заданием;
   - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

9.6. Контрольные вопросы

1. Какую информацию можно получить, воспользовавшись командой определения состояния протокола STP для VLAN (на корневом и не на корневом устройстве)? Приведите примеры вывода подобной информации на устройствах.
2. При помощи какой команды можно узнать, в каком режиме, STP или Rapid PVST+, работает устройство? Приведите примеры вывода подобной информации на устройствах.
3. Для чего и в каких случаях нужно настраивать режим Portfast?
4. В чем состоит принцип работы агрегированного интерфейса? Для чего он используется?
5. В чём принципиальные отличия при использовании протоколов LACP (Link Aggregation Control Protocol), PAgP (Port Aggregation Protocol) и статического агрегирования без использования протоколов?
6. При помощи каких команд можно узнать состояние агрегированного канала EtherChannel?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1; 25].

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155.

2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.

3. *A J.* Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_s.

4. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.

5. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.

6. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http://www.ietf.org/rfc/rfc3069.txt.

7. *Moy J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.

8. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.

9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.

10. *Neumann J. C.* Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.

11. *Odom S., Nottingham H.* Cisco Switching: Black Book. — The Coriolis Group, 2001. — ISBN 9781576107065. — URL: http://books.google.sk/books?id=GYsLAAAACAAJ.

12. *Tetz E.* Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html.

13. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: http://protect.gost.ru/v.aspx?control=7&id=132355.

14. *Кларк К., Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.

15. *Королькова А. В., Кулябов Д. С.* Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.

16. *Королькова А. В., Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.

17. *Королькова А. В., Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.

18. *Королькова А. В.*, *Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.

19. *Куроуз Д. Ф.*, *Росс К. В.* Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

20. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.

21. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

22. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.

23. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.

24. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science). — ISBN 978-5-496-00831-0.

25. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.

26. Цикл статей «Сети для самых маленьких». — URL: `http://linkmeup.ru/blog/11.html`.

27. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: `https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html`.