

СПИСОК ЛИТЕРАТУРЫ

1. Касаткин В.В., Колбанев М.О., Татарникова Т.М. Предметная область информационного взаимодействия//В сборнике: Региональная информатика и информационная безопасность Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2015. С. 260-264.
2. Project Management Institute. 2010. A Guide to the Project Management Body of Knowledge (Pmbok Guide): Official Russian Translation (Russian Edition).
3. Фунтов В.Н. Основы управления проектами в компании. Учеб. пособие. 4-е изд. - СПб.: Питер, 2018. 464 с.

УДК 004.94

РАЗРАБОТКА МОДЕЛЕЙ ПРОТОКОЛОВ СЕМЕЙСТВА FHRP В СРЕДЕ OMNET++

Носков Илья Игоревич

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский, пр., 49, Санкт-Петербург, 197101, Россия
e-mail: noskovii@mail.ru

Аннотация. Рассмотрена среда имитационного моделирования компьютерных сетей OMNeT++, а также ее возможности по моделированию семейства протоколов FHRP (First Hop Redundancy Protocol), обеспечивающих клиентов отказоустойчивым шлюзом. Описан подход к построению моделей отказоустойчивых сетевых протоколов, позволяющий проектировать компьютерные сети высокой доступности.

Ключевые слова: моделирование; компьютерные сети; FHRP; отказоустойчивость; OMNeT++.

DEVELOPING OF FHRP MODELS IN OMNET++

Noskov Ilya

Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
(University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mail: noskovii@mail.ru

Abstract. The simulation environment of computer networks OMNeT ++ is considered. The paper describes process of simulation FHRP (First Hop Redundancy Protocol) protocols in the OMNeT++ environment. Technique for creation of network simulation models is considered. The paper describes simulation models of fault tolerance computer networks protocols, which allows designing high availability computer networks.

Keywords: modeling; computer networks; FHRP; fault-tolerance; OMNeT++.

Введение.

Экономическая эффективность предприятий в условиях цифровой экономики во многом определяется безопасностью [1-6], надежностью и отказоустойчивостью [7-9] инфокоммуникационных систем и сетей и организации взаимодействия в них прикладных программ различной функциональной направленности [10].

Развитие сетевого оборудования и каналов связи позволяет передавать данные на скоростях в несколько терабит в секунду. Вместе с тем растет количество потребителей трафика и сервисов с высоким уровнем доступности, а также сервисов, предоставляющих услуги в максимально короткий промежуток времени (банковские операции, транзакции, системы реального времени), в которых даже секундные перебои могут привести к потере актуальности информации и сбою в работе. В связи с данными факторами возрастает потребность в построении отказоустойчивых компьютерных сетей [11, 12], предоставляющих свои услуги с минимальной задержкой даже при отказе одного из элементов. Существует целое семейство протоколов FHRP (First Hop Redundancy Protocols), обеспечивающих отказоустойчивость маршрутизаторов путем объединения их в группу, представляющую собой виртуальный маршрутизатор, отказоустойчивость которого выше, чем отказоустойчивость каждого отдельного маршрутизатора, составляющего группу [13]. Для оценки работы и глубокого исследования данных протоколов хорошо подходит имитационное моделирование, которое позволяет проводить исследования сетей различной конфигурации путем построения их моделей без необходимости построения компьютерных сетей из реального оборудования [14-19]. Программные средства моделирования упрощают процесс принятия проектных решений построения распределенных компьютерных сетей, а также делают сам процесс проектирования менее затратным. Из данных факторов вытекает актуальность исследования и построения моделей отказоустойчивых компьютерных сетей, использующих в своей работе протоколы семейства FHRP.

К протоколам, обеспечивающим отказоустойчивость шлюзов семейства FHRP относятся как проприетарные реализации (HSRP, GLBP, SMLT), так и свободные реализации (VRRP, CARP). Данные протоколы хорошо описаны с теоретической точки зрения в различных статьях и документах, однако наблюдается нехватка научных статей с количественной оценкой работы данных протоколов, позволяющей сделать вывод об эффективности использования того или иного протокола в построении компьютерных сетей различной конфигурации. Компьютерное моделирование позволяет дать количественную оценку работы объектов, поведение которых моделируется. Для этого создается абстракция реального физического объекта в виртуальной среде, которая затем исследуется путем проведения экспериментов на компьютере (или

компьютерах, если речь идет о распределенном моделировании). В настоящее время существует огромное количество систем моделирования, которые в свою очередь делятся на универсальные и узкоспециализированные. К узкоспециализированным средствам моделирования компьютерных сетей относят такие средства как NS-3, OPNET и OMNeT++. Среда OMNeT++ является наиболее предпочтительной из представленных так как является кроссплатформенной, имеет богатую библиотеку сетевых компонентов и реализаций протоколов на языке C++, которые можно менять или разрабатывать свои, имеет графический интерфейс, а также подробную англоязычную документацию [19]. Среда моделирования компьютерных сетей OMNeT++ позволяет строить модели сетевых протоколов и устройств, используя при этом принцип композиции и усложнения моделей, выделения их в отдельный блок. Разработка моделей и их конфигурирование выполняется с помощью языка программирования C++ и встроенного языка описания сети NED. Также доступна возможность использования графического редактора при построении моделей.

В настоящее время для системы моделирования OMNeT++ разрабатывается много различных компонентов и протоколов программистами со всего мира. Наборы компонентов и протоколов объединяются в библиотеки, которые называются фреймворками. В настоящее время основным фреймворком для OMNeT++ является INET Framework, который поддерживается сообществом разработчиков OMNeT++. INET Framework является библиотекой с открытым исходным кодом, которая предоставляет модели проводных, беспроводных и мобильных сетей. Ниже представлен краткий список моделей, разработанных в рамках данной библиотеки [20]:

- модели канального уровня проводных и беспроводных сетей (Ethernet, PPP, IEEE 802.11 и т.д.);
- модели протоколов IP-стека (TCP, UDP, IPv4, IPv6, OSPF, BGP и т.д.);
- модели MPLS-сетей (LDP, RSVP-TE и т.д.);
- реализация моделей и протоколов других уровней модели OSI (физический, канальный, сетевой, транспортный, приложений);
- поддержка IPv4/IPv6;
- протоколы маршрутизации.

Наличие такого большого количества готовых компонентов позволяет пользователю не заниматься реализацией сетевых протоколов согласно документам, RFC с помощью языка C++, а сосредоточиться на создании сетевых моделей и проведении экспериментов для дальнейших исследований.

Прежде чем начать моделирование протоколов семейства FHRP в среде OMNeT++ с использованием фреймворков, необходимо детально разобраться с самим механизмом работы данных протоколов. Протоколы семейства FHRP реализуют механизмы сетевой отказоустойчивости в современных компьютерных сетях путем обеспечения балансировки нагрузки между несколькими маршрутами в сети и высокой доступности шлюзов, заданных по умолчанию, за счет их дублирования и совместной работы, а также гарантируют очень быстрое время восстановления в случае аварий [21]. В рамках работы данных протоколов маршрутизаторы объединяются в так называемую «виртуальную группу», которой назначается один «виртуальный» IP-адрес. Таким образом, в каждый момент времени клиенты работают только с одним маршрутизатором из группы. При отказе основного маршрутизатора всю работу по обслуживанию клиентов берет на себя резервный маршрутизатор, причем для клиентов это делается абсолютно прозрачно, т.к. виртуальный адрес остается тот же, несмотря на то, что трафик от клиента будет идти уже через другое физическое устройство. На рис. 4 приводится схема, использующая протокол семейства FHRP и 2 маршрутизатора, объединенных в группу и с заданным виртуальным адресом для нее:

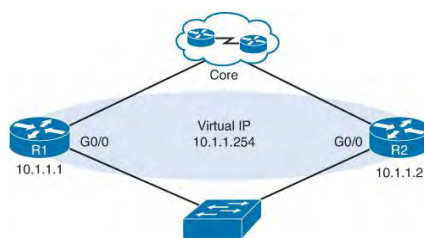


Рис. 4. FHRP-схема резервирования маршрутизаторов

Семейство протоколов FHRP включает в себя свободные реализации (VRRP, CARP) и проприетарные (HSRP, SMLT, GLBP), которые используются ведущими вендорами сетевого оборудования (Cisco, Juniper Networks). Моделирование различных конфигураций компьютерных сетей, использующих данные протоколы для обеспечения отказоустойчивости шлюзов, позволит выделить преимущества и недостатки того или иного протокола из всего семейства и выбрать наиболее подходящий из них для использования в необходимой схеме без физического проектирования сети и проведения экспериментов на реальном сетевом оборудовании, что позволит сократить время и средства на проектирование компьютерных сетей.

Фреймворк ANSAINET расширяет рассмотренную ранее библиотеку INET в части разработки протоколов для проводных сетей. ANSAINET также является проектом с открытым исходным кодом. Данный фреймворк предоставляет следующие основные возможности/улучшения относительно INET Framework [22]:

- новая модель маршрутизатора, которая представляет собой совокупность более простых компонентов, реализующих определенную функциональность;
- протоколы семейства FHRP (HSRP, VRRPv2, GLBP);

маршрутизаторы, входящие в одну группу. Для хоста маршрут по умолчанию прописывается через адрес виртуального маршрутизатора, в данном случае через 192.168.1.254.

В ini файле модели описываются начальные состояния объектов, а также описывается алгоритм моделирования и задается время прогона. В данном случае мы запускаем утилиту ring на хосте, которая проверяет доступность маршрутизатора по виртуальному адресу, заданному для группы VRRP-маршрутизаторов.

В файле scenario.xml описываются два периодических события – разрыва и восстановления соединения между коммутатором и вторым VRRP-маршрутизатором. Разрыв связи с маршрутизатором как раз запускает процесс в рамках протокола VRRP, который идентифицирует отказ и назначает главным маршрутизатором другое устройство из той же группы. Утилита ring продолжает проверять доступность виртуального маршрутизатора, однако обрабатывает эти запросы уже другой маршрутизатор из группы. Факт переключения маршрутизаторов для клиента остается прозрачным.

После создания модели компьютерной сети и задания всех настроек пользователь может запустить выполнение моделирования в интерактивном сеансе и наблюдать весь процесс работы сети в реальном времени. По окончании эксперимента пользователю становятся доступны результаты в виде статистической информации и логов событий процесса моделирования. Данный подход к построению моделей отказоустойчивых компьютерных сетей подходит и для других протоколов, таких как HSRP и GLBP, которые также базируются на объединении маршрутизаторов в «виртуальные группы».

Заключение.

Выработан подход к имитационному моделированию протоколов семейства FHRP по обеспечению сети отказоустойчивым шлюзом с использованием фреймворка ANSAINET в среде моделирования OMNeT++ . Описаны основные возможности и архитектура некоторых компонентов среды моделирования. Детально описан процесс построения моделей, их конфигурирования, моделирования и анализа результатов. Предложенный подход проведения имитационного моделирования компьютерных сетей со встроенными механизмами протоколов обеспечения сетевой отказоустойчивости шлюзов позволяет в дальнейшем продолжить изучение механизмов обеспечения отказоустойчивости в компьютерных сетях, а также строить более сложные и специфичные модели сетей для их дальнейшего анализа.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т. М. Задача синтеза комплексной системы защиты информации в ГИС // Ученые записки Российского государственного гидрометеорологического университета. 2013. № 30. С. 204-211.
2. Верзун Н.А., Колбанёв М.О., Татарникова Т.М. Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности Санкт-Петербург, 2016. С. 52-56
3. Коломойцев В.С. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос. 2015. № 3. С. 71-79
4. Коршунов И.Л., Пуха Г.П. Концепция построения защищенного комплекса для формирования и распределения нагрузки вуза // Информационная безопасность регионов России. 2015. С. 219-220
5. Емельянов А.А., Коршунов И.Л. Опыт реализации политики информационной безопасности на предприятии малого бизнеса в целях обеспечения информационно-экономической безопасности // Информационная безопасность регионов России. 2015. С. 213-214.
6. Татарникова Т.М. Аналитико-статистическая модель оценки живучести сетей с топологией mesh // Информационно-управляющие системы. 2017. № 1 (86). С. 17-22.
7. Богатырев В.А., Богатырев С.В. Критерии оптимальности многоустойчивых отказоустойчивых компьютерных систем // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2009. № 5(63). С. 92-98
8. Богатырев В.А., Богатырев А.В., Голубев И.Ю., Богатырев С.В. Оптимизация распределения запросов между кластерами отказоустойчивой вычислительной системы // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3(85). С. 77-82
9. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4(86). С. 150-151
10. Пуха Г.П., Драчёв Р.В., Попцова Н.А. Информационно-логическая модель базы данных для системы интеллектуальной поддержки принятия решений. Известия вузов Приборостроение. 2017. Т. 60. № 2. С. 117-124
11. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация древовидной сети с резервированием коммутационных узлов и связей // Телекоммуникации. 2013. № 2. С. 42-48
12. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения // Информационные технологии. 2013. № 2. С. 27-32
13. Носков И.И. Протоколы обеспечения сетевой отказоустойчивости информационных экономических систем // Информационно-технологическое обеспечение цифровой экономики: сборник статей сотрудников кафедры информационных систем и технологий - 2018. - С. 66-72
14. Головкин Ю.Б., Гусаренко А.С. Моделирование производственных систем в GPSS // Управление в сложных системах. Межвузовский научный сборник. Уфимский государственный авиационный технический университет. Уфа. 2011. С.136-149
15. Татарникова Т.М., Яготинцева Н.В. Вероятностная модель установления соединения в инфокоммуникационной сети // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 157-166.
16. Богатырев В.А., Богатырев С.В. Своевременность обслуживания в многоуровневых кластерных системах с поэтапным уничтожением просроченных запросов // Вестник компьютерных и информационных технологий - 2018. - № 2(164). - С. 28-35
17. Богатырев В.А., Богатырев С.В. Резервированное обслуживание в кластерах с уничтожением неактуальных запросов // Вестник компьютерных и информационных технологий. 2017. № 1(151). С. 21-28
18. Богатырев В.А., Богатырев С.В. Надежность мультикластерных систем с перераспределением потоков запросов // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. - № 2. С. 171-177
19. Хабаров С.П. Моделирование Ethernet сетей в среде OMNeT++ INET framework // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 3. С. 462-472. doi: 10.17586/2226-1494-2018-18-3-462-472
20. What Is INET Framework? // [Электронный ресурс] – Режим доступа: <https://inet.omnetpp.org/Introduction.html>, свободный. – Загл. с экрана.
21. Носков И.И. Методы и алгоритмы обеспечения надежности и отказоустойчивости компьютерных сетей // Синергия Наук. 2018. № 24. С. 603-616
22. ANSAINET extends INET framework for OMNeT++ // [Электронный ресурс] – Режим доступа: <https://ansa.omnetpp.org/>, свободный. – Загл. с экрана.