УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2019 Том 19 № 4 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTCS
July–August 2019 Vol. 19 No 4 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004.94 doi: 10.17586/2226-1494-2019-19-4-673-679

МОДЕЛИРОВАНИЕ КОМПЬЮТЕРНОЙ СЕТИ С ОТКАЗОУСТОЙЧИВЫМ ШЛЮЗОМ В СРЕДЕ OMNeT++

И.И. Носков

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: noskovii@mail.ru

Информация о статье
Поступила в редакцию 04.04.19, принята к печати 30.04.19
Язык статьи — русский

Ссылка для цитирования: Носков И.И. Моделирование компьютерной сети с отказоустойчивым шлюзом в среде OMNeT++ // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 4. С. 673–679. doi: 10.17586/2226-1494-2019-19-4-673-679

Аннотация

Предмет исследования. Обеспечение отказоустойчивости шлюзов в компьютерных сетях с использованием семейства протоколов FHRP. Дано описание протоколов FHRP и среды моделирования компьютерных сетей OMNeT++. Показан процесс создания имитационной модели в среде OMNeT++ с использованием библиотеки ANSA-INET. Приведено детальное описание алгоритма работы протокола HSRP и описание возможностей его исследования и изучения путем моделирования в среде OMNeT++. **Цель работы.** Исследование процесса построения моделей компьютерных сетей с отказоустойчивым шлюзом в среде OMNeT++ на примере протокола HSRP. **Метод.** Предлагаемый подход к изучению протоколов обеспечения отказоустойчивости шлюза в компьютерных сетях основан на проведении имитационных экспериментов в среде моделирования. Показаны возможности в разработке компьютерных сетей, работающих на базе протоколов семейства FHRP, в среде OMNeT++ при использовании фреймворка ANSA-INET, содержащим большую библиотеку готовых сетевых моделей, компонентов и реализаций протоколов. Дано краткое описание процесса создания модели и основных возможностей фреймворка ANSA-INET в части моделирования протоколов обеспечения отказоустойчивости шлюзов. **Основные результаты.** Разработана модель компьютерной сети с кластером маршрутизаторов, на каждом из которых запущен протокол HSRP, который позволяет выполнять резервирование маршрутизатора, являющегося шлюзом в сети. Разработана модель компьютерной сети с отказоустойчивым шлюзом. Представлена методика разработки моделей компьютерных сетей, использующих протоколы семейства FHRP для реализации механизма отказоустойчивого шлюза. Описаны основные этапы разработки модели и ее исполнения. **Практическая значимость.** Представленные в данной работе результаты могут быть использованы при построении надежных компьютерных сетей, обеспечивающих бесперебойную работу при отказе сетевого шлюза. Описанные в данной работе инструментарий и алгоритм создания моделей позволяют проводить исследования отказоустойчивости шлюзов компьютерных сетей, а также строить системы автоматизированного проектирования надежных компьютерных сетей.

Ключевые слова
компьютерные сети, имитационное моделирование, отказоустойчивость, шлюз, FHRP, HSRP, OMNeT++, ANSA-INET

doi: 10.17586/2226-1494-2019-19-4-673-679

MODELING OF COMPUTER NETWORK WITH FAULT-TOLERANCE GATEWAY IN OMNeT++

I.I. Noskov

ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: noskovii@mail.ru

Article info
Received 04.04.19, accepted 30.04.19
Article in Russian

For citation: Noskov I.I. Modeling of computer network with fault-tolerance gateway in OMNeT++. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 3, pp. 673–679 (in Russian). doi: 10.17586/2226-1494-2019-19-4-673-679

Abstract

Subject of Research. The paper considers the issues of providing fault-tolerance gateways in computer networks with the use of First Hop Redundancy Protocols (FHRP). The description of FHRP family protocols and simulator OMNeT++ is given. The process of simulation model creation in OMNeT++ using ANSA-INET library is described. Detailed description of HSRP algorithm

is presented and researching opportunities for simulation study by OMNeT++ simulator are considered. **Work Objective.** The aim of the work is the study of computer network models creation with fault-tolerance gateway in OMNeT++ simulator on the HSRP protocol example. **Method.** The proposed approach to the study of FHRP protocols in computer networks is based on carrying out simulation experiments in simulation environment. We show development potential for computer networks based on FHRP protocols in OMNeT++ using ANSA-INET framework which contains a large library of completed network models, components and protocol implementations. The paper describes in brief the process of computer network model development and ANSA-INET framework main abilities concerning the modeling of fault-tolerance gateways. **Main Results.** Computer network model with routers cluster is developed. Every router works with HSRP protocol. It gives the possibility to perform a router redundancy, that is a gateway in this computer network. Simulation model of computer network with fault-tolerance gateway is developed. We present the method of developing computer network models using FHRP protocols for fault-tolerance gateway implementation. The main stages of model development and completion are described. **Practical Relevance.** The presented results can be used in the design of high-reliable and fault-tolerance computer networks providing continuity of service at network gateway failure. The described tools and algorithm for development of computer network models give the possibility to carry out research on gateway fault-tolerance in computer networks and create computer-aided design systems for reliable computer networks.

Keywords
computer networks, simulation modeling, fault-tolerance, gateway, FHRP, HSRP, OMNeT++, ANSA-INET

Введение

Использование распределенных компьютерных сетей различного назначения позволяет решать различные вычислительные задачи, а также предоставляет транспортную инфраструктуру для передачи данных из одной точки в другую, расположенных на территориальном удалении друг от друга. При использовании компьютерных сетей в системах реального времени (СРВ) или для организации сервисов с высоким уровнем доступности сбои в работе каналов связи или сетевого оборудования могут привести к различным негативным последствиям (финансовые потери, утрата актуальности передаваемой информации или же к трагическим последствиям в случае отказа СРВ) [1–3]. Надежность современных распределенных систем обработки информации достигается путем резервирования ресурсов хранения, передачи и обработки данных, при этом используется кластеризация серверов и агрегирование каналов связи. Дополнительные возможности повышения надежности дает динамическое распределение запросов с учетом деградации системы [4, 5]. Для систем реального времени, в том числе в кластерных системах многопутевой маршрутизации [6–9], функциональная надежность может быть повышена на основе резервированного обслуживания копий запросов [10]. Исследование возможностей резервирования обслуживания копий запросов, критичных к задержкам ожидания в одноуровневых и многоуровневых кластерах и системах многопутевой передачи представлено в работах [11, 12].

Зачастую в компьютерных сетях на уровне ядра сети организуются механизмы обеспечения надежности путем использования многопутевой маршрутизации, построения отказоустойчивых топологий или с помощью сетевых протоколов [13]. Однако граничные маршрутизаторы, к которым непосредственно подключены пользовательские сети обычно не защищены должным образом, что приводит к потерям важной информации еще до пересылки ее в сеть более высокого уровня. Так, например, при отказе шлюза в локальной компьютерной сети трафик от всех клиентов данной сети будет теряться неопределенное количество времени до момента восстановления работы оборудования, что является критичным для рассмотренных ранее систем.

В настоящее время существуют протоколы сетевого уровня, позволяющие строить сети с отказоустойчивым шлюзом, обеспечивая тем самым надежность передачи данных из локальной сети во внешнюю. Данные протоколы относятся к протоколам семейства FHRP (First Hop Redundancy Protocol). Актуальной является задача исследования работы данных протоколов в различных сетевых конфигурациях, изучение специфики и особенности работы каждого из них для возможности дальнейшего проектирования компьютерных сетей с отказоустойчивым шлюзом. Для решения данной задачи подходит имитационное моделирование, так как оно позволяет не строить физические сети, а значит, исключает финансовые затраты и экономит время.

Протоколы семейства FHRP

Семейство протоколов FHRP позволяет строить компьютерные сети с отказоустойчивым шлюзом путем объединения физических маршрутизаторов или L3-коммутаторов в кластер, представляющий собой виртуальный маршрутизатор, на который назначается виртуальный IP-адрес и MAC-адрес (Media Access Control). В каждый момент времени на ARP-запросы (Address Resolution Protocol) по данному виртуальному IP-адресу от клиентов, желающих передавать трафик, отвечает одно из устройств кластера, выбранного в данный момент в качестве «главного», либо же осуществляется балансировка нагрузки и трафик передается через несколько маршрутизаторов. При отказе «главного» маршрутизатора в кластере осуществляется выбор нового «главного» устройства, которое возьмет на себя работу виртуального маршрутизатора, обеспечив тем самым отказоустойчивость шлюза, представленного кластером.

К протоколам, обеспечивающим отказоустойчивость шлюзов семейства FHRP (First Hop Redundancy Protocol), относятся как проприетарные реализации (HSRP (Hot Standby Router Protocol), GLBP (Gateway

Load Balancing Protocol)), так и свободные реализации (VRRP (Virtual Router Redundancy Protocol), CARP (Common Address Redundancy Protocol)) [14]. HSRP является одним из протоколов данного семейства и разработан компанией Cisco Systems. Затем на основе HSRP был создан протокол Virtual Router Redundancy Protocol (VRRP), у которого есть некоторые проблемы с патентными правами, так как он основан на HSRP. Протокол Common Address Redundancy Protocol (CARP) был разработан в 2003 г. командой разработчиков операционной системы OpenBSD и не имеет проблем с патентными правами. В отличие от рассмотренных протоколов семейства FHRP протокол Gateway Load Balancing Protocol (GLBP) помимо обеспечения отказоустойчивости шлюза, также предоставляет балансировку нагрузки за счет того, что он работает в режиме Active/Active вместо Active/Standby, в котором работают все остальные протоколы[1].

Балансировка нагрузки достигается за счет того, что «главный» маршрутизатор присваивает каждому физическому устройству дополнительный виртуальный MAC-адрес. При ARP-запросе общего виртуального IP-адреса «главный» маршрутизатор в качестве ответа посылает один из MAC-адресов пассивных устройств, обеспечивая тем самым распределение нагрузки по всем маршрутизаторам кластера.

Среда моделирования компьютерных сетей OMNeT++

Моделирование компьютерных сетей предоставляет большие возможности для разработки и исследования сетей различной топологии и размера [15]. В настоящее время разработано существенное количество сред моделирования компьютерных сетей. Среда моделирования OMNeT++ является мощным кроссплатформенным инструментом создания и исследования моделей компьютерных сетей различного назначения [16]. Данная среда имеет огромную библиотеку готовых компонентов и реализаций сетевых протоколов, что позволяет достаточно быстро строить и исследовать различные сетевые конфигурации. Среда написана на языке C++, что позволяет людям, знакомым с программированием, дорабатывать ее ядро и создавать собственные компоненты и библиотеки. Строить модели в среде OMNeT++ можно в графическом интерфейсе или с помощью описания модели в файлах с расширением .net, которые имеют Си-подобный синтаксис.

Для построения модели компьютерной сети с отказоустойчивым шлюзом, работающем на базе одного из протоколов семейства FHRP, необходимо использовать специально разработанный фреймворк ANSA-INET, который расширяет возможности среды OMNeT++ в части моделирования работы компьютерных сетей с использованием протоколов семейства FHRP, протоколов динамической и мультикаст маршрутизации[2]. Ниже представлен список основных компонентов и моделей, разработанных в рамках данной библиотеки ANSA-INET [17–19]:

— новая модель маршрутизатора, которая представляет собой совокупность более простых компонентов, реализующих определенную функциональность;

— протоколы семейства FHRP (HSRP, VRRPv2, GLBP);

— алгоритмы динамической маршрутизации (IS-IS, RIPv2, RIPng, EIGRP, Babel);

— протоколы управления L2-уровнем (CDP, LLDP);

— протоколы мультикаст маршрутизации (PIM-DM, PIM-SM, IGMPv2, IGMPv3).

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 графиков и наборов данных с полной трассировкой событий моделирования.

Протокол HSRP

Для исследования работы протоколов семейства FHRP рассмотрим протокол HSRP, который обеспечивает отказоустойчивость шлюза в локальной компьютерной сети. Данный протокол объединяет маршрутизаторы в так называемую HSRP-группу. Во время работы протокола выбирается активный маршрутизатор или маршрутизирующий коммутатор третьего уровня, выполняющий роль виртуального маршрутизатора и обеспечивающий пересылку пакетов из одной подсети в другую, остальные же маршрутизаторы или маршрутизирующие коммутаторы третьего уровня выполняют роли резервных виртуальных маршрутизаторов, ожидающие отказа активного маршрутизатора в рамках одной HSRP-группы[3].

В промежуток времени таймера приветствия (Hello Time) маршрутизаторы, находящиеся в одной HSRP-группе, ожидают пакеты приветствия (Hello Packet), которые посылает активный маршрутизатор. По истечении таймера удержания (Hold Time) резервный маршрутизатор посылает пакет, в котором содержится информация об отказе активного маршрутизатора, тем самым осуществляет приоритетное прерывание в группе и берет на себя роль активного маршрутизатора.

Выборы проводятся на основании приоритета маршрутизатора, который может изменяться в пределах от 1 до 255. Приоритет может быть назначен вручную, что позволяет влиять на процесс выбора. Если

[1] https://www.opennet.ru/base/cisco/cisco_hsrp_glbp.txt.html

[2] https://ansa.omnetpp.org/

[3] http://xgu.ru/wiki/HSRP

системный администратор не определил приоритет, используется значение по умолчанию, равное 100. 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. В процессе работы активный (active) и резервный (standby) маршрутизаторы обмениваются hello-сообщениями.

HSRP-протокол реализован поверх стека протоколов TCP/IP, для доставки служебной информации используется протокол UDP (User Datagram Protocol). Маршрутизаторы или маршрутизирующие коммутаторы, на которых сконфигурирован и функционирует протокол HSRP, в рамках обмена служебной информацией используют так называемые пакеты приветствия (hello packets). В свою очередь данные пакеты отправляются на IP-адрес групповой рассылки (multicast) 224.0.0.2 (HSRP Version 1) или на 224.0.0.102 (HSRP Version 2) по протоколу UDP на порт 1985[1].

Разработка модели компьютерной сети с отказоустойчивым шлюзом

Приступим к разработке модели и самому процессу моделирования работы протокола HSRP в среде OMNeT++ для изучения механизмов его работы. На рис. 1 показана исследуемая сеть, построенная в среде OMNeT++.

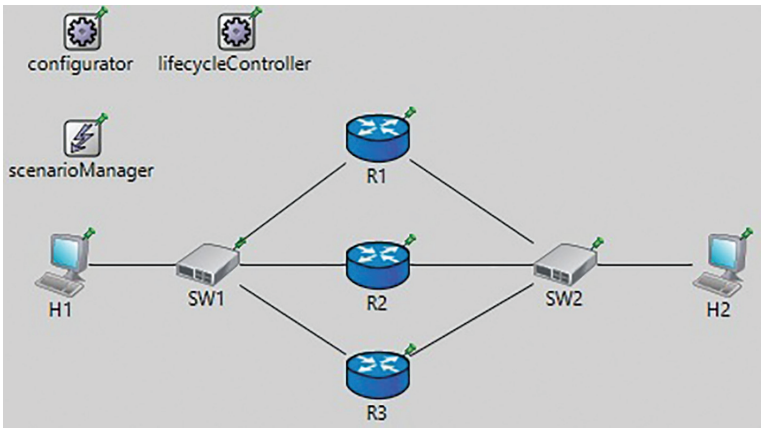

Рис. 1. Модель исследуемой компьютерной сети в среде OMNeT++

H1 и H2 являются клиентами, SW1 и SW2 — коммутаторами локальных сетей клиентов, а R1, R2 и R3 являются маршрутизаторами, которые могут работать с протоколом HSRP (рис. 1). Маршрутизаторы представляют собой модуль фреймворка ANSA-INET под названием ANSA_HSRPRouter, который представляет собой маршрутизатор, способный работать с протоколом HSRP.

Конфигурация элементов модели задается в файле config.xml. На рис. 2 приведены фрагменты сетевой конфигурации маршрутизаторов HSRP-группы и конфигурации клиентов.

```
            </HSRP>
        </Interface>
        <Interface name="eth1">
            <IPAddress>192.168.2.2</IPAddress>
            <Mask>255.255.255.0</Mask>
        </Interface>
    </Interfaces>
</Router>

<!--    R3      -->
<Router id="R3">
    <Interfaces>
        <Interface name="eth0">
            <IPAddress>192.168.1.3</IPAddress>
            <Mask>255.255.255.0</Mask>
            <HSRP>
                <Group ip="192.168.1.254" priority = "200"></Group>
            </HSRP>
        </Interface>
        <Interface name="eth1">
            <IPAddress>192.168.2.3</IPAddress>
            <Mask>255.255.255.0</Mask>
        </Interface>
    </Interfaces>
</Router>
```

```
<Host id="H1">
    <Interfaces>
        <Interface name="eth0">
            <IPAddress>192.168.1.5</IPAddress>
            <Mask>255.255.255.0</Mask>
        </Interface>
    </Interfaces>
    <DefaultRouter>192.168.1.254</DefaultRouter>
</Host>

<Host id="H2">
    <Interfaces>
        <Interface name="eth0">
            <IPAddress>192.168.2.5</IPAddress>
            <Mask>255.255.255.0</Mask>
        </Interface>
    </Interfaces>
    <DefaultRouter>192.168.2.254</DefaultRouter>
</Host>
```

Рис. 2. Конфигурации маршрутизаторов и клиентов

[1] http://www.adminia.ru/cisco-hsrp-nastroyka/

Из рис. 2 видно, что помимо IP-адресов физических интерфейсов маршрутизаторов задан их виртуальный адрес, а также указан приоритет маршрутизаторов, который будет использован при выборе активного маршрутизатора HSRP-группы. Для клиентов также указаны IP-адреса их сетевых интерфейсов.

Сам алгоритм моделирования описывается в файле omnetpp.ini. На рис. 3 показан фрагмент данного файла, в котором описана конфигурация генератора и потребителя трафика для клиентов, работа которых необходима для создания нагрузки на исследуемую сеть и изучение работы протокола HSRP.

```
**.H1.numUdpApps = 1
**.H1.udpApp[0].typename = "UDPBasicApp"
**.H1.udpApp[0].destAddresses =  "192.168.2.5"
**.H1.udpApp[0].destPort = 1000
**.H1.udpApp[0].messageLength = 100B
**.H1.udpApp[0].startTime = 40s
**.H1.udpApp[0].sendInterval = uniform(1s,2s)

**.H2.numUdpApps = 1
**.H2.udpApp[0].typename = "UDPSink"
**.H2.udpApp[0].localPort = 1000
```

Рис. 3. Настройка генератора и потребителя трафика клиентов

Для проверки работы протокола HSRP был создан скрипт scenario.xml, в котором моделируется отказ канала связи, соединяющего клиента H1 с маршрутизатором R3, который изначально выбран, как активный (так как имеет наибольший приоритет). На рис. 4 приведен фрагмент данного скрипта.

```
<scenario>
    <at t="50">
        <disconnect src-module="R3" src-gate="ethg$o[0]" />
        <disconnect src-module="SW1" src-gate="ethg$o[2]" />
    </at>

    <at t="100">
        <connect src-module="SW1" dest-module="R3" src-gate="
        <connect src-module="R3" dest-module="SW1" src-gate="
    </at>
</scenario>
```

Рис. 4. Фрагмент сценария, имитирующего отказ канала связи

На 50 секунде генерируется событие обрыва канала связи, а на 100 секунде канал восстанавливается. При этом после обрыва передача данных должна осуществляться по другому маршрутизатору из HSRP-кластера, чем и обеспечивается отказоустойчивость шлюза. Для проверки данного предположения запустим модель на выполнение и в режиме реального времени посмотрим на работу исследуемой компьютерной сети. На рис. 5 изображен процесс моделирования до обрыва канала связи.

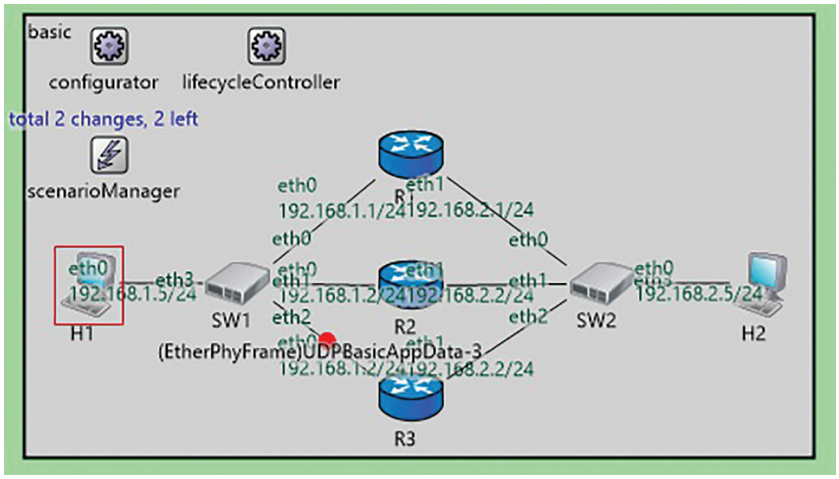

Рис. 5. Процесс моделирования до отказа канала связи

Из рис. 5 видно, что фрейм передается через маршрутизатор R3, представляющий собой активный маршрутизатор HSRP-группы согласно его приоритету. Состояние сети после отказа канала связи между клиентом H1 и маршрутизатором R3 показано на рис. 6.

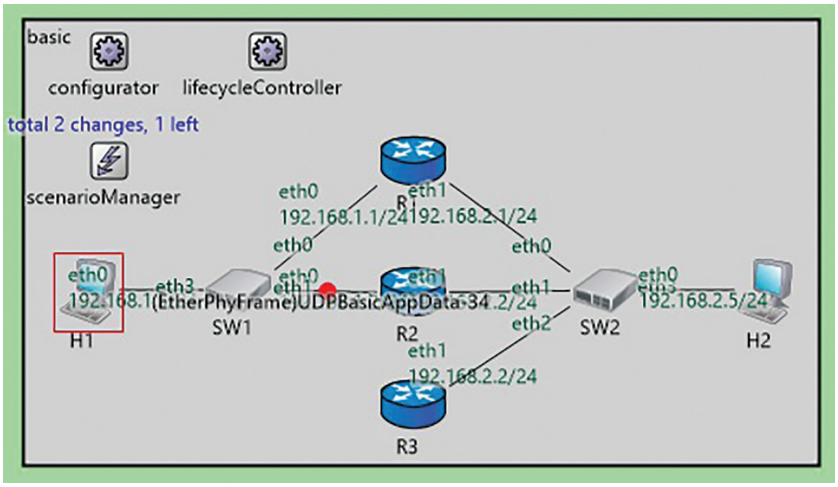

Рис. 6. Процесс моделирования после отказа канала связи

Согласно результатам моделирования, фреймы от клиента H1 сейчас передаются через маршрутизатор R2, который был выбран активным на основе его приоритета. Таким образом, в данной сети осуществляется отказоустойчивость шлюза, и при сбое одного из маршрутизаторов происходит выбор другого активного маршрутизатора из кластера, который берет на себя работу по пересылке данных.

Заключение

В результате проделанной работы было дано описание алгоритмов семейства FHRP, позволяющих строить компьютерные сети с отказоустойчивым шлюзом. Дано детальное описание работы алгоритма HSRP, а также среды моделирования компьютерных сетей OMNeT++.

В рассмотренной среде моделирования разработана модель компьютерной сети с отказоустойчивым шлюзом, реализованным с помощью протокола HSRP. Представлен подробный алгоритм построения и параметризации разработанной модели в OMNeT++. Приведен процесс моделирования и показано влияние параметров работы алгоритма на процесс реализации отказоустойчивости шлюза путем переключения работы на резервный маршрутизатор. Результаты работы, полученные в данной статье, могут быть полезны для дальнейшего исследования отказоустойчивости шлюзов компьютерных сетей, а также сетевым администраторам и инженерам.

Литература

1. Gunnar A., Johansson M. Robust load balancing under traffic uncertainty — tractable models and efficient algorithms // Telecommunication Systems. 2011. V. 48. N 1-2. P. 93–107. doi: 10.1007/s11235-010-9336-9
2. Aysan H. Fault-Tolerance Strategies and Probabilistic Guarantees for Real-Time Systems. Vasteras, Sweden, Malardalen University, 2012. 190 p.
3. Koren I., Krishna C.M. Fault Tolerant Systems. San Francisco: Morgan Kaufmann Publishers, 2009. 378 p.
4. Merindol P., Pansiot J., Cateloin S. Improving load balancing with multipath routing // Proc. 17th Int. Conf. on Computer Communications and Networks. St. Thomas, USA, 2008. P. 54–61. doi: 10.1109/icccn.2008.ecp.30
5. Rajeev V., Muthukrishnan C.R. Reliable backup routing in fault tolerant real-time networks // Proc. 9th Int. Conf. on Networks. Bangkok, Thailand, 2001.doi: 10.1109/icon.2001.962338
6. Sorin D. J. Fault Tolerant Computer Architecture. Morgan & Claypool, 2009. 103 p.
7. Veselý V., Rek V., Ryšavý O. Enhanced interior gateway routing protocol with IPv4 and IPv6 support for OMNeT++ / In: Simulation and Modeling Methodologies, Technologies and Applications. Springer, 2015. P. 65–82. doi: 10.1007/978-3-319-26470-7_4
8. Veselý V., Ryšavý O., Švéda M. Protocol independent multicast in OMNeT++ // Proc. 10th Int. Conf. on Networking and Services. Chamonix, France, 2014. P. 132–137.
9. Veselý V., Švéda M. L2 protocols in OMNeT++ / In: IP Networking 1 — Theory and Practice. Zilina: Zilina University Publ., 2012. P. 37–40.

References

1. Gunnar A., Johansson M. Robust load balancing under traffic uncertainty — tractable models and efficient algorithms. *Telecommunication Systems*, 2011, vol. 48, no. 1-2, pp. 93–107. doi: 10.1007/s11235-010-9336-9
2. Aysan H. *Fault-Tolerance Strategies and Probabilistic Guarantees for Real-Time Systems*. Vasteras, Sweden, Malardalen University, 2012, 190 p.
3. Koren I., Krishna C.M. *Fault Tolerant Systems*. San Francisco, Morgan Kaufmann Publishers, 2009, 378 p.
4. Merindol P., Pansiot J., Cateloin S. Improving load balancing with multipath routing. *Proc. 17th Int. Conf. on Computer Communications and Networks*. St. Thomas, USA, 2008, pp. 54–61. doi: 10.1109/icccn.2008.ecp.30
5. Rajeev V., Muthukrishnan C.R. Reliable backup routing in fault tolerant real-time networks. *Proc. 9th Int. Conf. on Networks*. Bangkok, Thailand, 2001.doi: 10.1109/icon.2001.962338
6. Sorin D.J. *Fault Tolerant Computer Architecture*. Morgan & Claypool, 2009, 103 p.
7. Veselý V., Rek V., Ryšavý O. Enhanced interior gateway routing protocol with IPv4 and IPv6 support for OMNeT++. In *Simulation and Modeling Methodologies, Technologies and Applications*. Springer, 2015, pp. 65–82. doi: 10.1007/978-3-319-26470-7_4
8. Veselý V., Ryšavý O., Švéda M. Protocol independent multicast in OMNeT++. *Proc. 10th Int. Conf. on Networking and Services*. Chamonix, France, 2014, pp. 132–137.
9. Veselý V., Švéda M. L2 protocols in OMNeT++. In *IP Networking 1 — Theory and Practice*. Zilina, Zilina University Publ., 2012, pp. 37–40.

10. Zhang Y., Fang Z., Xu Z. An optimal design of multi-protocol label switching networks achieving reliability requirements // Reliability Engineering & System Safety. 2019. V. 182. P. 133–141. doi: 10.1016/j.ress.2018.10.015
11. Богатырев В.А., Богатырев А.В. Модель резервированного обслуживания запросов реального времени в компьютерном кластере // Информационные технологии. 2016. Т. 22. № 5. С. 348–355.
12. 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.
13. 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. doi: 10.17586/0021-3454-2017-60-2-171-177
14. Богатырев С.В., Богатырев В.А. Объединение резервированных серверов в кластеры высоконадежной компьютерной системы // Информационные технологии. 2009. № 6. С. 41–47.
15. 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. doi: 10.14489/vkit.2017.01.pp.021-028
16. Кельтон В., Лоу А. Имитационное моделирование. 3-е изд. СПб.: BHV, 2004. 847 с.
17. Носков И.И. Разработка моделей протоколов семейства FHRP в среде OMNeT++ // Региональная информатика и информационная безопасность. 2018. № 5. С. 238–241.
18. Носков И.И., Богатырев В.А., Сластихин И.А. Имитационная модель локальной компьютерной сети с агрегированием каналов и случайным методом доступа при резервировании передач // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1047–1053. doi: 10.17586/2226-1494-2018-18-6-1047-1053.
19. Шувалов В.П., Егунов М.М., Минина Е.А. Обеспечение показателей надежности телекоммуникационных систем и сетей. М.: Горячая линия — Телеком, 2015. 168 с.

10. Zhang Y., Fang Z., Xu Z. An optimal design of multi-protocol label switching networks achieving reliability requirements. *Reliability Engineering & System Safety*, 2019, vol. 182, pp. 133–141. doi: 10.1016/j.ress.2018.10.015
11. Bogatyrev V.A., Bogatyrev A.V. The model of redundant service requests real-time in a computer cluster. *Informacionnye Tehnologii*, 2016, vol. 22, no. 5, pp. 348–355. (in Russian)
12. Bogatyrev V.A., Bogatyrev A.V., Golubev I.Yu., Bogatyrev S.V. Queries distribution optimization between clusters of fault-tolerant computing system. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 3, pp. 77–82. (in Russian)
13. Bogatyrev V.A., Bogatyrev S.V. Reliability of multi-cluster systems with redistribution of the flow of requests. *Journal of Instrument Engineering*, 2017, vol. 60, no. 2, pp. 171–177. (in Russian) doi: 10.17586/0021-3454-2017-60-2-171-177
14. Bogatyrev V.A., Bogatyrev S.V. Association reservation servers in clasters highly reliable computer system. *Informatsionnye Tekhnologii*, 2009, no. 6, pp. 41–47. (in Russian)
15. Bogatyrev V.A., Bogatyrev S.V. Redundant service clusters with the destruction of irrelevant queries. *Herald of Computer and Information Technologies*, 2017, no. 1, pp. 21–28. (in Russian) doi: 10.14489/vkit.2017.01.pp.021-028
16. Law A.M., Kelton W.D. *Simulation Modeling and Analysis*. McGraw-Hill, 1991.
17. Noskov I.I. Developing of FHRD models in OMNeT++. *Regional'naya Informatika i Informatsionnaya Bezopasnost'*, 2018, no. 5, pp. 238–241. (in Russian)
18. Noskov I.I., Bogatyrev V.A., Slastikhin I.A. Simulation model of local computer network with channel aggregation and random access method at redundant transfer. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1047–1053 (in Russian). doi: 10.17586/2226-1494-2018-18-6-1047-1053.
19. Shuvalov V.P., Egunov M.M., Minina E.A. *Reliability Indicators Providing of Telecommunication Systems and Networks.* Moscow, Goryachaya Liniya — Telekom Publ., 2015, 168 p. (in Russian)

Автор

Носков Илья Игоревич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-5489-4092, noskovii@mail.ru

Autors

Ilya I. Noskov — postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-5489-4092, noskovii@mail.ru