УДК 004.715

Методика внедрения неисправностей для анализа работы протокола резервирования бортового маршрутизатора

Брехов О.М.*, Балян А. В.**

Московский авиационный институт (национальный исследовательский университет), МАИ, Волоколамское шоссе, 4, Москва, А-80, ГСП-3, 125993, Россия

**e-mail: obrekhov@mail.ru*

***e-mail: balyanarm@gmail.com*

Аннотация

Центральным устройством бортовых сетей является маршрутизатор, который обеспечивает соединение бортовых сетей с внебортовыми. Для обеспечения отказоустойчивой связи используется протокол связи с маршрутизатором горячего резерва (Hot Standby Router Protocol HSRP). Основной задачей и предназначением данного протокола является достижение высокого уровня доступности и отказоустойчивости маршрутизатора. В данной работе предлагается подход, для анализа функционирования данного протокола, с использованием техники внедрения неисправностей. Основой данного подхода является имитация дополнительного маршрутизатора в HSRP группе, для реализации разных сценариев неисправностей. Неисправности внедряются в HSRP-группу и анализируется поведение протокола под их воздействием. Рассмотрены возможные отказы в системе и методы их внедрения.

Ключевые слова: отказоустойчивость**,** внедрение неисправностей, протокол HSRP.

Введение

В бортовых сетях летательных аппаратов маршрутизатор являются центральным устройством, обеспечивающим, взаимодействие с летным экипажем, наземным экипажем, бортовыми и наземными сетями. Его главной задачей является обеспечение межсетевой связи, а также выхода во внешнюю сеть для экипажа и пассажиров, играя роль шлюза [1]. Следовательно, отказ шлюза по умолчанию приведет к прекращению нормальной работы сети. Для достижения высокого уровня доступности шлюза по умолчанию используются протоколы резервирования. Данные протоколы должны обеспечивать отказоустойчивую связь узлов внутренней сети со шлюзом по умолчанию и, соответственно, обеспечить надёжный выход во внешнюю сеть. Важной задачей является тестирование и анализ функционирования протокола. Для понимания актуальности данной работы, были проанализированы существующие работы в данной области.

Все подходы анализа функционирования протоколов можно разделить на следующие: подходы на основе сетевых мониторов и фильтров и подходы с использованием внедрения неисправностей. Первая концепция не соответствует поставленной цели, т.к. она подразумевает анализ сети под воздействием реалистичного трафика и не дает понимания функционирования под воздействием сбоев и отказов.

В рамках второй концепции были разработаны разные методики и инструменты ([2], [3], [4], [5], [7]). Также есть разные подходы, которые используют

внедрение неисправностей на уровне аппаратуры [6]. Однако, т.к. нашими условиями было предусмотрено не изменять протокол и систему, а также независимость от операционной системы и топологии сети, то данные инструменты не соответствуют нашим условиям. Нашим требованиям соответствует Mendosus [8]. Последний не может эмулировать работу маршрутизаторов, также типы неисправностей, которые можно внедрять при помощи данного инструмента, не соответствуют нашим требованиям. Mendosus может внедрять ошибки портов, сетевых плат, коммутаторов. Второй инструмент Virtual-Wire [9], который дает возможность выполнять сброс, задержку, переупорядочивание, изменение, дублирование пакетов. Он не поддерживает топологию с резервированными устройствами, которая нужна для настройки и функционирования протокола HSRP, являющегося целью нашего исследования.

В данной работе разработан подход для анализа следующих пунктов.

- функционирование протокола HSRP в реальных условиях под воздействием сбоев и отказов
- выявление ошибок проектирования и настройки HSRP
- выявление нарушений в работе протокола HSRP по сравнению со спецификацией

Также к разрабатываемому подход, после анализа существующих работ, были предъявлены следующие требования - система и протокол, которые необходимо

протестировать не должны изменяться, подход должен быть независим от операционной системы (ОС) и количества маршрутизаторов в HSRP группе.

В данной работе рассматривается протокол HSRP, т. к. он был основой для разработки других протоколов резервирования первого перехода, таких как VRRP, CARP. Группа маршрутизаторов, работающих под управлением протокола HSRP, создают иллюзию одного виртуального маршрутизатора для подключенных узлов. Один из маршрутизаторов из группы выбирается для пересылки пакетов, которые приходят с узлов. Данный маршрутизатор называется активным. Другой маршрутизатор выбирается в качестве резервного, для выполнения функций активного маршрутизатора, в случае его отказа. Остальные маршрутизаторы находятся в состоянии прослушивания и следят за работой активного и резервного. Для уменьшения сетевого трафика только активный и резервный маршрутизаторы отправляют периодичные пакеты, сообщающие об их состоянии.

Для достижения поставленной цели используется методика внедрения неисправностей. Имитируется дополнительный маршрутизатор и внедряются разные сценарии неисправностей.

Работа построена следующим образом: во второй части рассматривается работа протокола HSRP, в третей части предлагаемый подход, в четвертой части приводятся экспериментальные результаты, в завершающей части рассмотрены существующие работы и приведены выводы.

Принцип работы HSRP

Данный протокол служит для обеспечения максимальной доступности шлюза по умолчанию [10]. Маршрутизаторы, на которых настроен протокол, объединяются в одну группу HSRP и имитируют работу одного виртуального маршрутизатора. В одной группе HSRP должны присутствовать *активный* маршрутизатор, который в настоящее время пересылает пакеты виртуального маршрутизатора, *резервный* маршрутизатор, который является первым кандидатом на замену активного и маршрутизаторы в состоянии прослушивания, которые не пересылают пакеты о своем состоянии и в случае необходимости тоже могут участвовать в выборах активного или резервного.

Во время работы, для сигнализации о состоянии маршрутизаторов, активный и резервный маршрутизаторы пересылают следующие типы сообщений

- приветствие (Hello) - передаваемое для индикации работы маршрутизатора и его способности работать в активном или резервном режиме.
- переворот (Coup) - передается в тех случаях, когда маршрутизатор “хочет” стать активным.
- отказ (Resign) - передается в тех случаях, когда маршрутизатор больше “не хочет” быть активным.

В работе протокола и во времени восстановления после отказа, важную роль играют таймеры. Таймер приветствия, который контролирует промежуток времени, в течение которого маршрутизаторы, находящиеся в рамках одной HSRP группы, ожидают пакеты приветствия от активного маршрутизатора и таймер удержания, который показывает время (в секундах), в течение которого сохраняется

корректность текущего приветствия. В случае истечения данного времени, маршрутизатор не отправивший пакет приветствия, считается неисправным и выбирается другой на его место. Значение данных таймеров задается при настройке протокола. Выбор данных параметров имеет существенное значение на время восстановления связи.

Выбор активного и резервного маршрутизаторов производится согласно их приоритетам. При сравнении приоритетов двух различных маршрутизаторов активным назначается тот, у которого значение приоритета выше. Вторая версия данного протокола поддерживает также отслеживание состояний внешних портов маршрутизаторов. В случае отказа внешнего порта приоритет маршрутизатора падает на 10 делений и на его место выбирается маршрутизатор с более высоким приоритетом.

Функционирование протокола под воздействием сбоев и отказов

Для достижения поставленной цели, предлагается метод внедрения неисправностей (ВН). Данный метод был предложен в [11] и предполагает внедрение разного рода реалистичных неисправностей в систему и анализ поведения системы под воздействием сбоев и отказов. В данной работе рассматривается топология с n количеством маршрутизаторов, состоящих в одной или нескольких HSRP группах Рисунок 1.

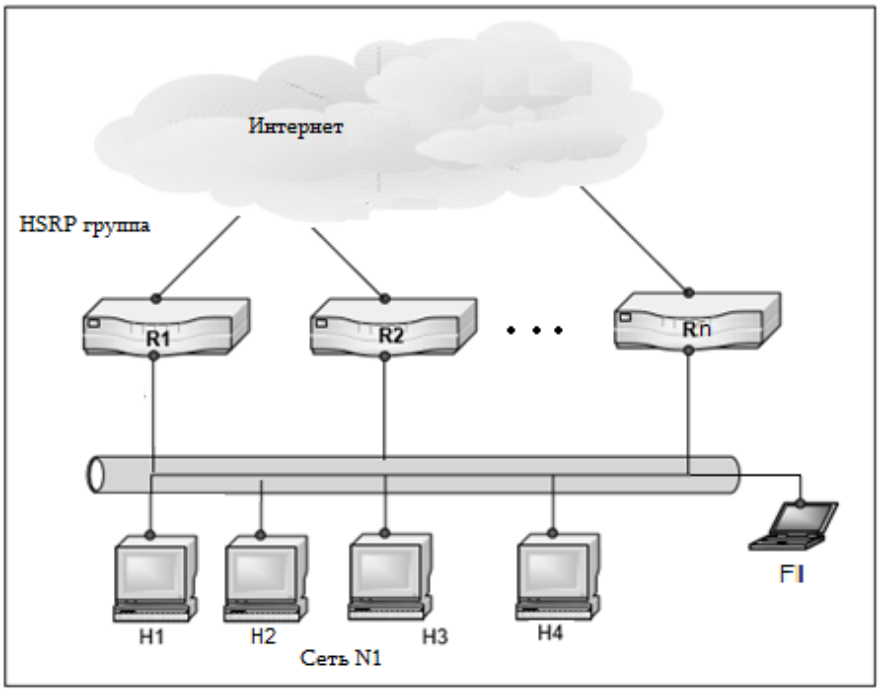

Рисунок 1 - Топология сети

Все возможные неисправности в маршрутизаторах, таких как крах операционной системы, критические неисправности на аппаратном уровне, выключение питания и.т.д, приводят к потере связи и, следовательно, их можно обобщить. В работе рассматриваются неисправности портов и линий связи.

1. f0 – отказ маршрутизатора R1
2. f1 –отказ порта R1 связывающего с сетью N1
3. f2 – отказ порта R1 связывающего с внешней сетью

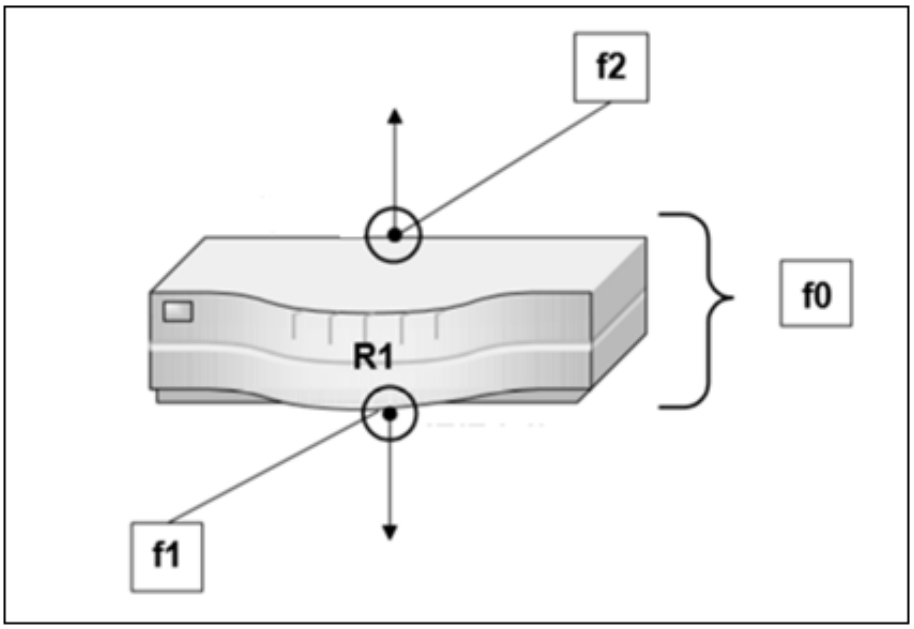

Рисунок 2 - Возможные неисправности

Так как в случае отказа портов и линий связи (в обоих случаях прерывается связь и не доходят пакеты приветствия) с f1 можно обобщить отказ линии связи с сетью N1, а с f2 - отказ линии связи с внешней сетью. Так как существующие методы и инструменты имеют программные компоненты, которые невозможно установить на маршрутизатор для проведения экспериментов ВН, то в данной работе предлагается имитация неисправностей маршрутизаторов, портов и линий связи при помощи дополнительного узла.

Описание подхода имитации маршрутизатора

Согласно топологии на рисунке 1, программа на узле FI генерирует HSRP пакеты и имитирует работу дополнительного маршрутизатора в группе. Таким образом, он становится членом HSRP группы и в соответствии со сценарием генерирует пакеты, выставляя себя на место активного, резервного,

прослушивающего или даже комбинируя состояния, имитирует работу и активного и резервного, отправляя пакеты с разных IP адресов. Поскольку, только активный и резервный маршрутизаторы рассылают пакеты приветствия, группа HSRP имеет представление только об их состоянии. Следовательно, для анализа функционирования протокола, нам необходимо внедрить вышеуказанные отказы f1, f2, f3 для активного и резервного маршрутизаторов. Узел FI может генерировать разные HSRP пакеты и влиять на работу виртуального маршрутизатора. Рассмотрим таблицу возможных состояний в таблице 1.

Таблица 1

Отказы и возможности их имитации

Отказ	**Способ имитации**	**Действие протокола согласно спецификации**
Активный маршрутизатор f0,f1	Пакет приветствия с наивысшим приоритетом и с значением поля состояния «активный»	FI берет на себя функцию активного маршрутизатора
Отказ	**Способ имитации**	**Действие протокола согласно спецификации**
Активный маршрутизатор f2	Пакет COUP с приоритетом больше на 10 чем у активного	FI берет на себя функцию активного маршрутизатора
Резервный маршрутизатор f0,f1	Пакет приветствия с наивысшим приоритетом и с значением поля состояния «резервный»	FI берет на себя функцию резервного маршрутизатора
HSRP мусор	Узел FI отправляет пакеты с некорректными параметрами	Перегрузка маршрутизаторов в HSRP группе
Отказ активного	Узел FI в состоянии «активный»	Резервный маршрутизатор

маршрутизатора	перестает отправлять пакеты приветствия	из HSRP группы берет на себя функцию активного
Отказ резервного маршрутизатора	Узел FI в состоянии «резервный» перестает отправлять пакеты приветствия	Выбор нового резервного маршрутизатора в группе
Отказ активного и резервного маршрутизаторов одновременно	Узел FI имитирует работу активного и резервного и перестает слать пакеты	Члены HSRP группы выбирают активного и резервного маршрутизаторов

Экспериментальный анализ

Данная методика была протестирована на реальном оборудовании, с использованием 3-х маршрутизаторов Cisco серии 2801. В качестве узла использовался персональной компьютер с процессором Intel Pentium (R) (2.70 GHz). Были проведены эксперименты для тестирования предлагаемого подхода и анализа работы протокола. Для генерации пакетов использовалась среда Hyenae. Для анализа воздействия использовались анализаторы трафика tcpdump, Wireshark.

Настройка маршрутизатора R1

FastEthernet0/1 - Group 100 (version 2)
State is Standby
15 state changes, last state change 00:07:34
Virtual IP address is 192.168.0.1
Active virtual MAC address is 0000.0C9F.F064
Local virtual MAC address is 0000.0C9F.F064 (v2 default)
Hello time 15 sec, hold time 40 sec
Next hello sent in 0.609 secs
Preemption enabled
Active router is 192.168.0.26
Standby router is local
Priority 100 (default 100)
Track interface FastEthernet0/0 state Up decrement 10
Group name is hsrp-Fa0/1-100 (default)

Пример отправки пакета приветствия в состоянии «активный» каждые 3 секунды с IP адреса 192.168.0.5, номер группы 100, значение приоритета 120, виртуальный IP адрес 192.168.0.1

```
# hyenae -I 3 -a hsrp-hello -o active -s 11:22:33:44:55:66-192.168.0.5 \
  # -d 192.168.0.1 -z 120 -g 100 -e 3000
```

В течении эксперимента было проимитировано многократное падение активного маршрутизатора.

Ниже приводится таблица переходов маршрутизатора R1.

```
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Speak -> Standby
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Standby -> Active
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Active  -> Speak
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Speak -> Standby
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Standby -> Active
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 100 state Speak -> Standby
```

Как видно из таблицы переходов, при помощи предложенного подхода, можно внедрять разные отказы и анализировать работу протокола под их воздействием.

Заключение

Отказоустойчивость шлюза является важнейшим средством для надежной связи с внешними сетями. Протокол маршрутизатора горячего резервирования является одним из методов обеспечения данной цели. В настоящей работе была предложена методика для анализа функционирования протокола HSRP, был произведен экспериментальный анализ данной методики и протокола под воздействием сбоев и отказов. В результате проделанной работы отмечается, что данная методика соответствует требованиям, а именно: не зависит от ОС, не меняет

настройки и параметры системы, не зависит от выбранной топологии, количества маршрутизаторов и HSRP-групп.

Библиографический список

1. Кучерявый А. А. Бортовые информационные системы. - Ульяновск: УлГТУ, 2004. – 504 с.

2. David T. S. Automated Fault-Inject Based Dependability Analysis of Distributed Computer Systems Center for Reliable and High-Performance Computing, Coordinated Science Laboratory University of Illinois at Urbana-Champaign. March. 2000, pp. 201-215.

3. Scott D. Probing and Fault Injection of Protocol Implementations, PFI Real-Time computing laboratory Distributed Computing Systems, Proceedings of the 15th International Conference, Nov. 1995 pp: 351 – 359

4. Tsai T. K., Iyer R. K. FTAPE: A Fault Injection Tool to Measure Fault Tolerance IEEE Computer. 1997. 30. N 4. pp. 75-82.

5. Gustavo M. O., Sergio L. C. Dependability Evaluation of Distributed Systems through Partitioning Faultn Injection.Test Workshop (LATW), 2010 11th Latin American, 28-31 March 2010, pp. 1 – 6.

6. Carvalho J.A., Portugal P.J. Assessment of PROFIBUS networks using a fault injection framework. IEEE Computer. Sept. 2005, Vol 1, pp. 423

7. Rodrigues N., Sousa D., Silva L. A Fault-Injector Tool to Evaluate Failure Detectors in Grid-Services Making Grids, IEEE Computer Nov. 2008, pp. 261-271

8. Li X., Martin R. Mendosus: A SAN-Based Fault-Injection Test-Bed for the Construction of Highly Available Network Services, Proceedings of the 1st Workshop on Novel Uses of System Area Networks (SAN-1), 2002

9. De P., Neogi A. Virtual Wire: A Fault Injection and analysis Tool for Network Protocols, Proceeding ICDCS '03 Proceedings of the 23rd International Conference on Distributed Computing Systems IEEE Computer Society Washington, DC, USA 2003, p. 214.

10. T. Li, Cisco Hot Standby Router Protocol (HSRP), RFC 2281, March 1998. pp. 17

11. Arlat J., Aguera M., Amat L. Fault injection for dependability validation: A methodology and some applications, IEEE Trans. Software Eng., Sep. 1990 vol. 16, no. 2, pp. 166– 182.