Инженерный вестник Дона, №9 (2019)
ivdon.ru/ru/magazine/archive/N9y2019/6243

О повышении доступности шлюза по умолчанию в корпоративных сетях

А.Н. Земцов[1], *Зунг ХаньЧан*[2]

[1]*Волгоградский государственный технический университет*
[2]*Национальный экономический университет*

Аннотация: Рассматривается важная составляющая защиты и обеспечения доступности автоматизированных систем управления технологическими процессами – шлюз по умолчанию. Основной задачей проекта является минимизация времени конвергенции путем обеспечения высокой доступности критически важных объектов с целью гарантирования непрерывности связи центральногоуправления технологическими процессами с территориально распределенными объектами производства. Приводится анализ работы одного из технологических решений, а также оценки вероятности безотказной работы для шлюза по умолчанию с резервированием и без.
Ключевые слова:HSRP, отказоустойчивость, высокая доступность, отказ, конвергенция, маршрутизация, протокол, нагруженный резерв, резервирование, непрерывность бизнеса.

Рост влияния информационно-коммуникационных технологий на все области человеческой деятельности формирует более жесткие требования к показателям надежности современныхиндустриальных сетей, как составляющих критически важных объектов. Ранее функциональные системы критически важных объектов создавались изолированными от глобальной сети и на основе проприетарных протоколов и технологий. Технологические процессы современного предприятия требуют унификации и стандартизации используемых решений, что обуславливает массовый переход на новые поколения индустриальных сетей, а также применение подходов к обеспечению доступности, защите и резервированию автоматизированных систем управления технологическими процессами (АСУ ТП).Для крупных предприятий отказ сети всего в течение нескольких минут в год может привести к чрезвычайно крупным потерям[1], что делает актуальным исследования обеспечения отказоустойчивости сети предприятия, в том числе, процессов восстановления сети после сбоев и отказов[2]. Сбои и отказы важных инфраструктурных элементов

индустриальной сети могут существенно повлиять на продуктивность работы АСУ ТП целом[3].

Резервирование является эффективным и широко применяемым методом кардинального повышения показателей надежности в технических системах, в том числе, критически важных объектах, и функционирующих на нихАСУ ТП [4].Один из способов достичь этого заключается в использовании оборудования в режиме холодного резерва[5]. Однако, такой подход не обеспечивает непрерывности бизнеса.

Для обеспечения отказоустойчивости маршрутизации, в том числе, снижения времени конвергенции, могут использоваться современные технологические решения [6-8], которые основаны на виртуализации маршрутизаторов, заключающейся в объединении группы маршрутизаторов в виртуальный маршрутизатор, выполняющий роль шлюза по умолчанию.

Виртуальный маршрутизатор является абстрактным представлением активного маршрутизатора, а также одного, или нескольких, резервных маршрутизаторов, работающих в режиме нагруженного резерва замещением.Одним из таких решений является протокол HSRPкомпании Cisco, описанным в стандарте RFC 2281.

Группа HSRP имеет виртуальный IP-адрес, а также и виртуальный MAC-адрес, а активный маршрутизатор обеспечивает передачу пакетов, направленных хостами на шлюз по умолчанию.Конечные хосты используют протокол разрешения адресов ARP для разрешения MAC-адреса, связанного с IP-адресом шлюза по умолчанию. Активный маршрутизатор отвечает на запросы ARP виртуальным MAC-адресом группы. Кадры, которые отправляются на виртуальный MAC-адрес, физически обрабатываются активным маршрутизатором. Физический маршрутизатор, пересылающий трафик корпоративной сети в Интернет, скрыт от конечных хостов.

Активные и резервные маршрутизаторы выбираются во время процесса выборов. Процесс выбора основан на значении приоритета, которое настраивается на каждом маршрутизаторе в группе. Если все маршрутизаторы имеют одинаковый приоритет, активным маршрутизатором становится маршрутизатор с наибольшимIP-адресом. С момента запуска процесса HSRP маршрутизатор проходит через ряд состояний, прежде чем он становится активным маршрутизатором[6].

Для изучения процессов восстановления сети в случае отказов был разработан стенд, показанный на рисунке 1. Топология сети представлена 1 коммутаторомуровня 2, двумя коммутаторами уровня 3, маршрутизатором, и двумя конечными хостами. IP-адреса настроены на интерфейсах, как показано на рисунке 1.

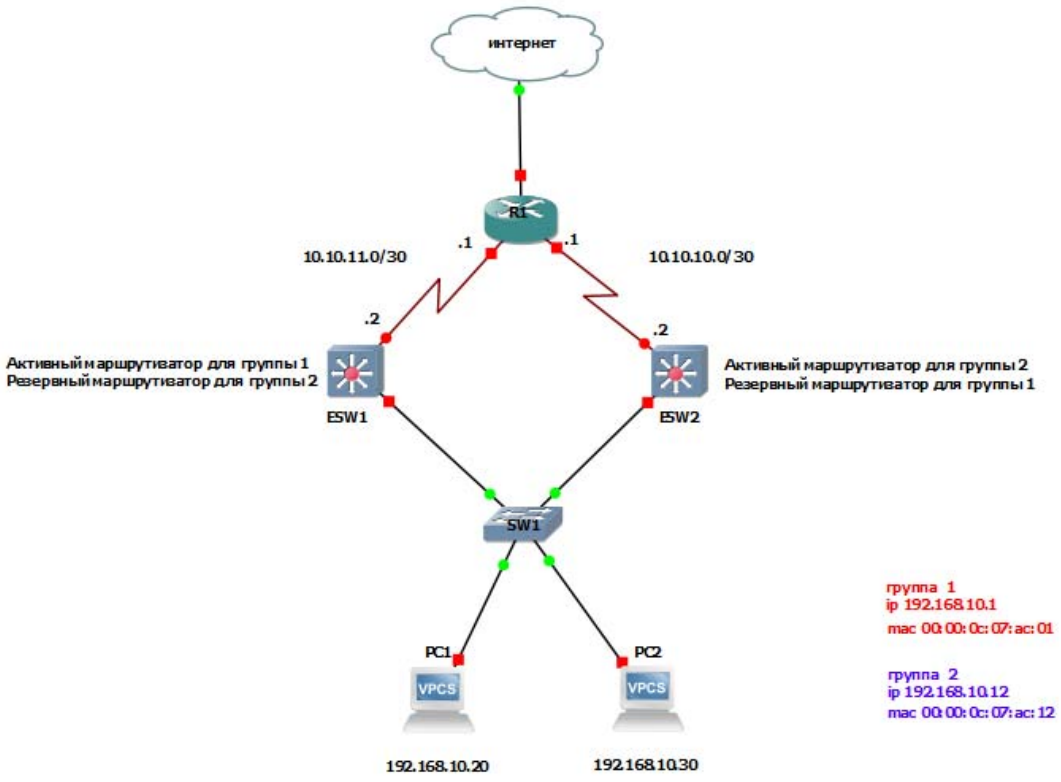

Рис. 1. – Топология исследовательского стенда.

В качестве шлюза по умолчанию PC1использовался виртуальный IP-адрес группы 1, а PC2был настроен с виртуальным IP-адресом группы 2 в

качестве шлюза. Для динамической маршрутизации пакетов между хостами использовался усовершенствованный дистанционно-векторный протокол динамической маршрутизации EIGRP. ESW1 был настроен в качестве активного маршрутизатора для группы 1 и в качестве резервного маршрутизатора для группы 2, а ESW2 – наоборот. Было использовано несколько конфигураций протокола HSRP, одна из которых приведена на рисунке 2.

Для представленного стенда вероятность безотказной работы [9] группы HSRPдля общего резервирования равнонадежных коммутаторов ESW1 и ESW2 с нагруженным резервом запишется как$P_{HSRP}(t) = 1 - \left(1 - p(t)\right)^2$, где $p(t)$ – вероятность безотказной работы коммутатора в течение времени t.Среднююнаработку на отказ предоставляет производитель, которая для данной популярной модели коммутаторов составляет 442000 часов.Легко найти, что вероятность безотказной работы коммутатора$p(t)$через 1 год, 2 года и 3 года составит 0.980376, 0.961137 и 0.942276, соответственно, а вероятность $P_{HSRP}(t)$– 0.999615, 0.998489 и 0.996534.

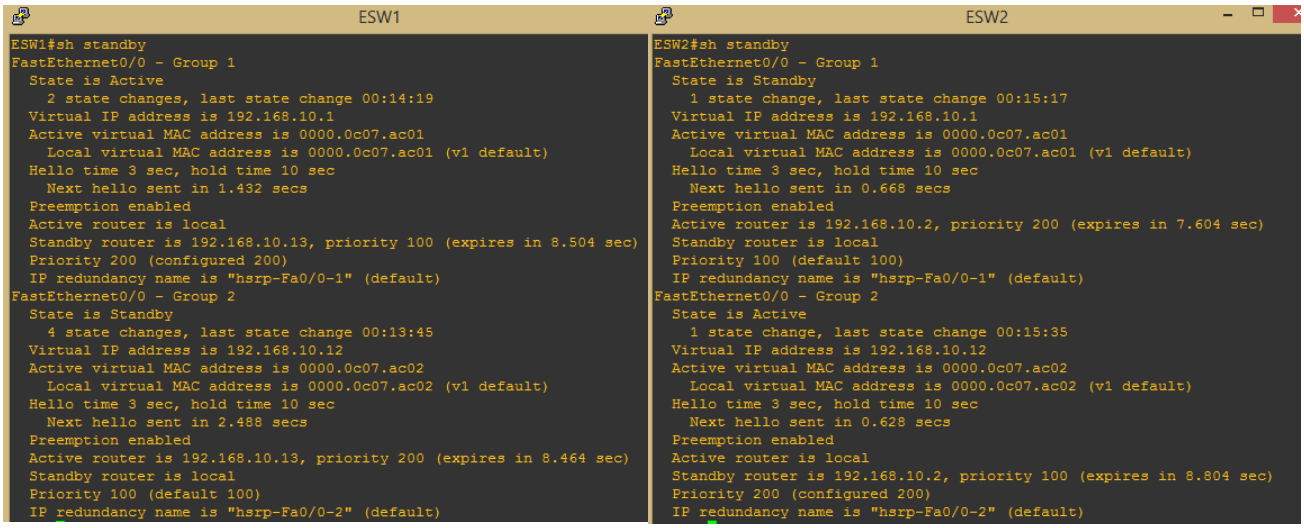

Рис. 2. – Конфигурация HSRP на маршрутизаторах ESW1 и ESW2.

Изучение процессов восстановления после отказов было проведенопутем одновременного теста доступности DNS-сервера Google по

IP-адресу 8.8.8.8 с PC1 и PC2. Пакеты ICMPмежду коммутаторами, PC1 и PC2были захвачены с помощью снифферaWireshark [10]. На рисунке 3 показано содержимое одного из ICMP-пакетов, переданных с PC1 на хост 8.8.8.8.

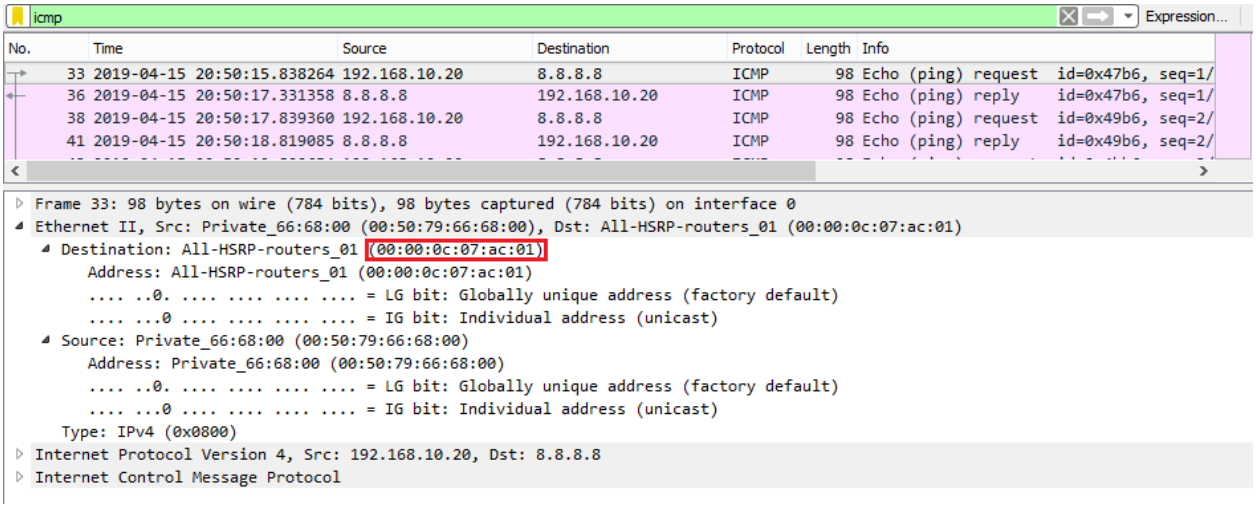

Рис. 3. – ICMP-пакет, переданный с PC1 на хост 8.8.8.8.

Как видно из захваченных пакетов, PC1 отправляет свой трафик через интерфейс с MAC-адресом 00:00:0c:07:ac:01, который является виртуальным MAC-адресом группы 1, в которой ESW1 имеет состояние Active.

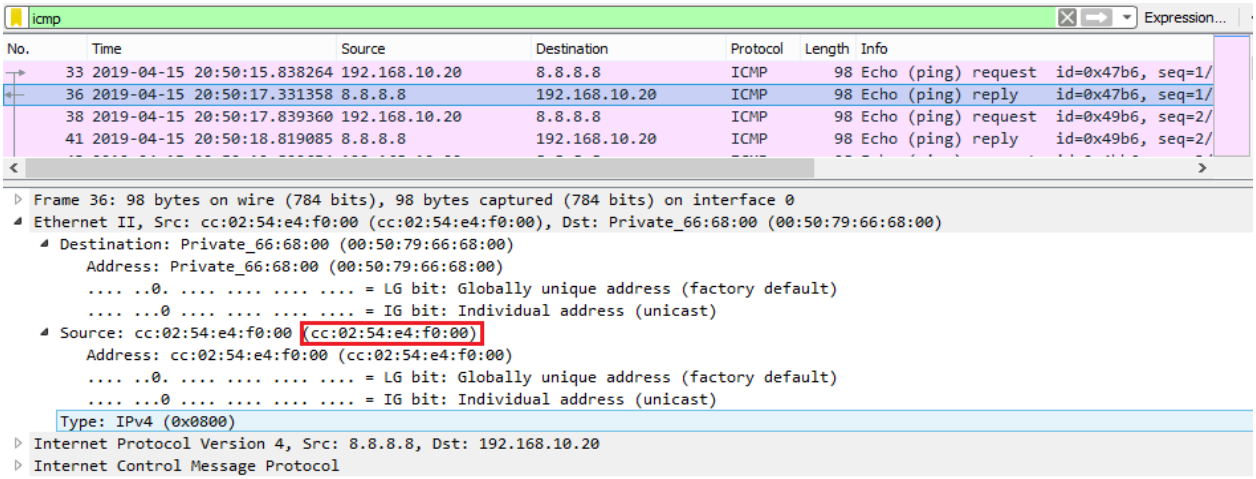

Рис. 4. – ICMP-ответ, переданный от хоста 8.8.8.8 на PC1.

Как видно на рисунке 4, PC1 получает свой трафик через интерфейс fastethernet 0/0 коммутатора ESW2 с MAC-адресом cc:02:54:e4:f0:00, которым он подключен к коммутатору SW1.

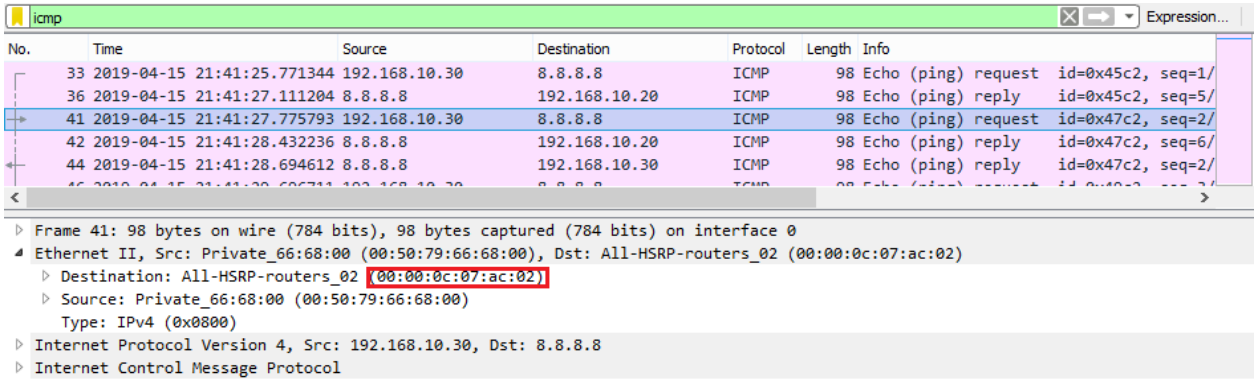

Рис. 5. – ICMP-пакет, переданный с PC2на хост 8.8.8.8.

На рисунке 5 показано, что PC2 отправляет свой трафик через интерфейс с MAC-адресом 00:00:0c:07:ac:12, который является виртуальным MAC-адресом группы 2, в которой ESW2 имеет состояние Active. Как видно на рисунке 6, PC2 получает свой трафик через интерфейс fastethernet 0/0 коммутатора ESW1 с MAC-адресом cc:01:5b:60:f0:00, которым он подключен к коммутатору SW1.

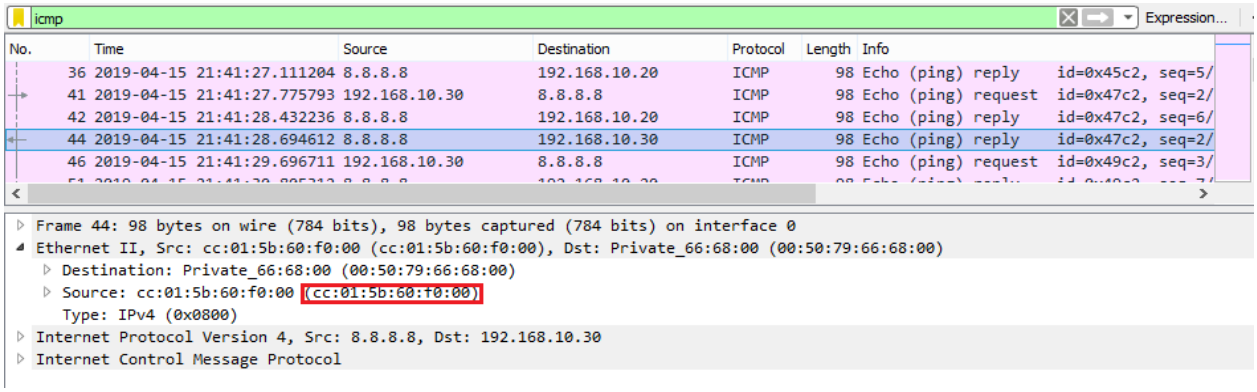

Рис. 6. – ICMP-ответ, переданный от хоста 8.8.8.8 на PC2.

Как видно на рисунке 6, PC2 получает свой трафик через интерфейс fastethernet 0/0 коммутатора ESW1 с MAC-адресом cc:01:5b:60:f0:00, которым он подключен к коммутатору SW1.

Результаты показывают, что оба маршрутизатора ESW1 и ESW2 используются для передачи пакетов, т.е. обеспечивают балансировку нагрузки. Работа резервных устройств в режиме ненагруженного резерва позволяет достичь лучших показателей надежности, по сравнению с нагруженным резервом, а также снизить расход потребляемой энергии.

Однако, необходимо учитывать, что работа резервных устройств в режиме ненагруженного резерва не обеспечивает приемлемое время конвергенции.

Литература

1. Пащенко У.Ю. Корпоративная сеть как инструмент повышения эффективности управления предприятием // Экономика и предпринимательство, 2018. №10 (99). С. 1250-1254.
2. Зотов А.И., Гриценко В.В., Черпаков А.В.Частичный отказ в теории надежности // Инженерный вестник Дона, 2018, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5350.
3. Шапошников, Д.Е. Применение принципа гарантированного результата для учёта качественной информации о предпочтениях при комплексной оценке качества функционирования телекоммуникационных сетей // Инженерный вестник Дона, 2014, № 4-1. URL: ivdon.ru/ru/magazine/archive/N4y2014/2574.
4. Tipper D. Resilientnetworkdesign: challengesandfuturedirections // TelecommunicationSystems, 2014. Vol. 56. pp. 5-16.
5. Каяшев А.И., Рахман П.А., Шарипов М.И.Анализ показателей надежности локальных компьютерных сетей // Вестник УГАТУ, 2014. Т.17. № 5(58). С. 140-149.
6. Макаренко С.И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности, 2015. №2. С. 45-98.
7. Girao-Silva R. Improving network availability - A design perspective // Third International Congress on Information and Communication Technology ICICT 2018, 2018. Vol.797.pp. 799-817.

8. Peralta J.A. High availability WAN implementation with MPLS to improve network connectivity in a financial institution// Lecture Notes in Engineering and Computer Science, 2017. pp. 47-50.
9. Гришко А.К.Определение показателей надежности структурных элементов сложной системы с учетом отказов и изменения параметров // Измерение. Мониторинг. Управление. Контроль, 2016. №2 (16). С. 51-57.
10. Батенков К.А. Анализ статистики трафика сети Ethernet с помощью программы Wireshark // Телекоммуникации, 2018. № 10. С. 39-48.

References

1. PashhenkoU.Ju. Jekonomika i predprinimatel'stvo, 2018. №10 (99). pp. 1250-1254.
2. ZotovA.I., GricenkoV.V., CherpakovA.V. Inzenernyj vestnik Dona, 2018, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5350.
3. Shaposhnikov, D.E. Inzenernyj vestnik Dona 2014, № 4-1. URL: ivdon.ru/ru/magazine/archive/N4y2014/2574.
4. Tipper D. Telecommunication Systems, 2014. Vol. 56. pp. 5-16.
5. Kajashev A.I., Rahman P.A., Sharipov M.I. Vestnik UGATU, 2014. T.17. № 5(58). pp. 140-149.
6. Makarenko S.I. Sistemyupravlenija, svjaziibezopasnosti, 2015. №2. pp. 45-98.
7. Girao-Silva R. Third International Congress on Information and Communication Technology ICICT 2018, 2018. Vol.797.pp. 799-817.
8. Peralta J.A. Lecture Notes in Engineering and Computer Science, 2017. pp. 47-50.
9. Grishko A.K. Izmerenie. Monitoring. Upravlenie. Kontrol', 2016. №2 (16). pp. 51-57.
10. Batenkov K.A. Telekommunikacii, 2018. № 10. pp. 39-48.