УДК 004.057.4

Время сходимости протоколов маршрутизации при отказах в сети

Макаренко С. И.

Постановка задачи: *увеличение структурной сложности сетей связи и рост интенсивности передаваемого трафика актуализирует вопросы обеспечения устойчивости сетей к отказам ее отдельных элементов - каналов и узлов связи. Проведенный анализ статистики причин отказов в сетях показал, что до 70% отказов обусловлены старением телекоммуникационного оборудования, 20% - некорректными операциями технического обслуживания, 17% - сбоями в программном обеспечении. При возникновении сетевого отказа протоколы маршрутизации должны обеспечить его корректную обработку, особенно если он ведет к изменению топологии сети, причем сделать это с минимальными временными затратами.* ***Целью работы*** *является анализ времени сходимости сети и оценка влияния на данное время различных факторов: временных параметров протоколов маршрутизации, сложности топологии сети, пропускной способности каналов связи и загрузки сети.* ***Используемые методы.*** *Анализ времени сходимости сети проводился на основе имеющихся публикаций по итогам исследований в этой предметной области. Проведен анализ статистики отказов и причин их возникновения. Проведен анализ протоколов, получивших распространение для внутридоменной маршрутизации. Показано, что наилучшие показатели по обеспечению сходимости сети обеспечивают протоколы на основе анализа состояния каналов, в связи с чем именно они были выбраны для дальнейшего рассмотрения. Проведен анализ временных параметров протокола маршрутизации и принципов его функционирования при отказе в сети, которые влияют на время сходимости. На основе этого анализа, рассмотрены и классифицированы основные технологические и протокольные решения, применяемые разработчиками сетевого оборудования для снижения времени сходимости. Представлен обзор результатов исследований времени сходимости сети для различных протоколов маршрутизации, топологий сетей и настроек временных параметров протоколов. Проведен сравнительный анализ значений времени сходимости при моделировании сетевых отказов в среде OPNET и проведении экспериментов на реальном телекоммуникационном оборудовании. В заключении статьи, на основе научных работ последних лет, проведен анализ направлений совершенствования протоколов маршрутизации в части улучшения их устойчивости к отказам в сети и снижения времени сходимости.* ***Новизна.*** *Элементом новизны работы является результаты обобщенного анализа принципов функционирования протоколов маршрутизации и влияния их временных параметров на время сходимости сети. Также к элементу новизны стоит отнести теоретическое обобщение направлений совершенствования протоколов маршрутизации в части улучшения их устойчивости к отказам в сети и снижения времени сходимости.* ***Результаты и их значимость.*** *Результаты обобщенного анализа принципов функционирования протоколов маршрутизации, а также влияния их временных параметров на время сходимости сети могут быть использованы для обоснования новых алгоритмических решений при маршрутизации трафика в сетях, на которые воздействуют различного рода дестабилизирующие факторы. Представленный в работе анализ перспективных направлений совершенствования протоколов маршрутизации может быть использован для совершенствования таких протоколов как: OSPF, OSPF-TE, IS-IS, IGRP, EIGRP. Кроме того, ряд рассматриваемых в статье решений может быть положен в основу разработки протоколов маршрутизации для мобильных MANET сетей, построенных на основе Mesh-технологий.*

Ключевые слова: *маршрутизация, внутридоменная маршрутизация, сходимость сети, время конвергенции, отказ в сети, OSPF, OSPF-TE, IS-IS, IGRP, EIGRP, MANET.*

Актуальность

Развитие современных сетей связи, высокие скорости передачи информации, а также высокие требования к надежности и устойчивости сетей актуализируют исследование процессов восстановления сетей после отказов.

Несмотря на то, что современное активное сетевое оборудование относится к высоконадежным элементам, отказы в сетях не так уж редки.

Проведенный анализ работ [1, 2] показал, что признаки отказов в сетях можно классифицировать по следующим пересекающимся группам:

- 45%...70% - естественное старение элементов аппаратного обеспечения маршрутизаторов (в первую очередь износом интерфейсных плат) [2];
- 20% - некорректные операции технического обслуживания [2];
- 17% - сбои в программном обеспечении маршрутизаторов [2, 3];
- 16% - сбоями в электропитании [3];
- применительно к транспортным сетям 84% отказов в них обусловлены сбоями оптического оборудования [4].

Каждый отказ в сети ведет к прекращению информационного обмена на десятки секунд. С учетом высоких скоростей передачи, это вызывает потери гигабит данных, и, как следствие, существенно снижает готовность сети.

Проведенный анализ работ отечественных авторов показал, что повышение устойчивости сетей связи к отказам ее элементов за счет реконфигурации информационных потоков и повышения эффективности протоколов маршрутизации является актуальной прикладной задачей. По данному направлению исследований ведут работу следующие ученые: Поповский В.В. [5-7], Лемешко А.В. [7-9], Романюк А.А. [9], Попков В.К. [10, 11], Блукке В.П. [11], Сорокин А.А. [12, 13], Дмитриев В.Н. [12, 13], Перепелкин Д. А. [14-17], Корячко В. П. [17], Мейкшан В.И. [18], Пасечников И.И. [19, 20], Громов Ю.Ю. [21], Ковальков Д.А. [22], Горбунов И.Э. [23], Егунов М. М. [24], Шувалов В. П. [24]. Однако в работах этих ученых не рассматривается временные параметры реакции протокола маршрутизации на отказ в сети, не детализируются процессы реконфигурации маршрутов, а основное внимание уделяется топологическим аспектам устойчивости сетей.

Проведенный автором анализ научных работ показал, практически полное отсутствие подробных исследований реакции протокола маршрутизации на отказы в сети, которые бы были опубликованы на русском языке. Поэтому основная часть представленного в работе анализа основана на публикациях зарубежных авторов. В рамках данной работы рассмотрены процессы реакции сети на отказы каналов связи и узлового оборудования в пределах одной автономной области маршрутизации, поэтому в ней анализируются только протоколы внутридоменной динамической маршрутизации. Работа развивает ранее опубликованные исследования автора в области анализа реакции протоколов OSPF [25] и EIGRP [26] на отказы в сети.

В общем случае протоколы внутридоменной динамической маршрутизации основаны на алгоритмах, которые можно отнести к одной из двух групп:

- дистанционно-векторные алгоритмы (DVA - Distance Vector Algorithm);
- алгоритмы состояния каналов (LSA - Link State Algoritm).

В протоколах на основе DVA каждый маршрутизатор периодически и широковещательно рассылает по сети сообщения, содержащие вектор, компонентами которого являются расстояния, измеренные в той или иной метрике от данного маршрутизатора до всех известных ему сетей. Получив от некоторого соседа вектор расстояний (дистанций) до известных тому сетей, маршрутизатор наращивает компоненты вектора на величину расстояния от себя до данного соседа. Обновленное значение вектора маршрутизатор рассылает своим соседям. Таким образом, в результате широковещательной рассылки каждый маршрутизатор узнает через смежные с ним маршрутизаторы информацию обо всех имеющихся в составной сети подсетях и о расстояниях до них. Дистанционно-векторные алгоритмы устойчиво функционируют только в небольших сетях. В больших сетях они могут загружать линии связи интенсивным широковещательным трафиком. Кроме того, изменения топологии сети могут не всегда корректно обрабатываться протоколами этого типа, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только косвенной информацией - вектором расстояний. К протоколам на основе DVA относятся: RIP, IGRP, EIGRP (гибридный), AODV.

В протоколах на основе LSA каждый маршрутизатор обладает данными о топологии сети. Используя данные о топологии, он вычисляет дерево кратчайших путей SPT (Shortest Path Tree) и на основе него составляет таблицу маршрутизации. Вычисление SPT ведется за счет использования алгоритма поиска кратчайших путей SPF (Shortest Path First), который, как правило, основан на алгоритме Дейкстры. В протоколе на основе состояния каналов предусмотрен регулярный обмен сообщениями о состоянии (метрике) канала связи и коррекции топологии сети. Вследствие того, что протоколы изначально ориентированы на учет данных о всей топологии сети, данный тип протоколов является гораздо более устойчивым. При этом протоколы на основе LSA обеспечивают меньшее время сходимости по сравнению с дистанционно-векторными протоколами маршрутизации. К протоколам на основе относятся IS-IS и OSPF.

Основные параметры протоколов внутридоменной динамической маршрутизации, а также междоменного протокола BGP (Border Gateway Protocol), представлены в таблице 1 по данным из работы [27].

Анализ функционирования протоколов внутридоменной динамической маршрутизации показал, что, несмотря на ряд различий, касающихся вычисления метрики путей в сети и алгоритмических подходов к вычислению кратчайших путей, общие принципы их функционирования применительно к реакции на отказы каналов весьма схожи. В связи с тем, что протоколы маршрутизации на основе алгоритмов состояния каналов обладают лучшими характеристиками по времени сходимости, в данной работе будет рассмотрен протокол OSPF, как наиболее распространенный представитель LSA протоколов. Кроме того, будет уделено внимание проприетарному гибридному протоколу EIGRP, обеспечивающему быстрое восстановление сети при отказах каналов связи.

Таблица 1 - Сравнительная таблица основных характеристик протоколов динамической маршрутизации [27]

Показатели/ протоколы	RIP v.2	IGRP	EIGRP	IS-IS	OSPF	BGP v.4
Безопасность	Открытый пароль или аутентификация по ключу MD5	–	Аутентификация по ключу MD5	–	Открытый пароль или аутентификация по ключу MD5	Разные методы аутентификации
Тип алгоритма	Вектор расстояния	Вектор расстояния	Комбини-рованный	Состояние каналов связи	Состояние каналов связи	Вектор расстояния
Балансировка нагрузки	–	Разные метрики	Разные метрики	Одинаковые метрики	Одинаковые метрики	Разные метрики (полу-автоматически)
Объединение маршрутов	–	–	+	–	+	+
Маски подсетей переем. длины	+	–	+	–	+	+
Максимальное количество машрутизаторов в сети	15	255 (реком. <50)	255	1024	65534	65534
Учет в метрике различных характеристик пути	Одна основная	Комбини-рованная	Комбини-рованная	Одна основная и три дополни-тельные	Одна основная и три дополни-тельные	Произвольная
Поддержка QoS	–	+	+	+	+	–
Обновления маршрутной информации	Вся таблица	Вся таблица	Только изменения	Только изменения	Только изменения	Только изменения
Необходимость логической подготовки сети	–	–	–	Выделение центральной области и связных областей	Выделение центральной области и связных областей	Разбитие сети на автономные системы и описание взаимодействия между ними
Доступность реализации	Открытый	Только на оборудова-нии Cisco Systems	Только на оборудова-нии Cisco Systems	Открытый	Открытый	Открытый
Поддержка IPv6	–	–	+	–	+	+

Анализ временных параметров протокола маршрутизации, определяющих время сходимости

Проведем исследование временных параметров, определяющих реакцию протокола маршрутизации на основе состояния каналов на сетевой отказ на примере протокола OSPF. Анализ работ [1, 28-30] позволил выявить основные параметры, влияющие на время сходимости в сети.

Процесс сходимости в сети состоит из следующих основных операций [1]:

1) обнаружение отказа элемента сети;
2) генерирование нового LSA-сообщения для оповещения о произошедшем изменении;
3) лавинная рассылка LSA-сообщений в сети;

4) выполнение алгоритма поиска кратчайших путей SPF на каждом маршрутизаторе, который получает LSA-сообщения;
5) обновление таблиц маршрутизации RIB/FIB на каждом маршрутизаторе по итогам пересчета SPF.

Время сходимости (*Convergence_Time*) определяется в соответствии с выражением [28]:

$$Convergence\_Time = Failure\_Detection\_Time + LSA\_Generation\_Time + Event\_Propagation\_Time + SPF\_Run\_Time + RIB\_FIB\_Update\_Time,$$

где:

- *Failure_Detection_Time* - время, необходимое для обнаружения отказа;
- *LSA_Generation_Time* – время генерации и начала рассылки LSA-сообщения об отказе элемента сети и изменении топологии;
- *Event_Propagation_Time* - время, необходимое для распространения LSA-сообщений о топологии всем маршрутизаторам в сети;
- *SPF_Run_Time* - время, необходимое для запуска алгоритма поиска кратчайших путей SPF после получения новых LSA-сообщений;
- *RIB_FIB_Update_Time* - время, необходимое для выполнения алгоритма SPF и обновления таблиц маршрутизации RIB/FIB.

Данные временные параметры, в свою очередь, определяются временными параметрами более низкого уровня, в связи с чем рассмотрим их более подробно.

Время, необходимое для обнаружения отказа на физическом уровне (*Failure_Detection_Time*). Для проверки работоспособности каналов связи и отношений собственной смежности маршрутизаторы обмениваются сообщениями Hello. В случае неполучения очередного Hello-пакета по какому-либо каналу связи, маршрутизатор переводит данный канал в режим ожидания восстановления связи. В случае если в течение времени *Dead_Interval* потеряны несколько Hello-пакетов подряд, то канал считается отказавшим и маршрутизатор генерирует LSA-сообщение об отказе канала. Таким образом, своевременность обнаружения отказа канала связи определяется следующими параметрами [28, 30, 32]:

- *Hello_Interval* – интервал обмена Hello-пакетами между смежными маршрутизаторами;
- *Dead_Interval* – интервал времени, в течение которого маршрутизатор ожидает восстановления связи в канале (получения очередного Hello-пакета). По истечению данного времени смежный маршрутизатор по данному каналу считается недоступным. Данный интервал, как правило, кратен значению *Hello_Interval*.

Значения OSPF по умолчанию: *Hello_Interval*=10 с, *Dead_Interval* =4·*Hello_Interval*=40 с.

При использовании способа обнаружения отказов на основе пакетов Hello, максимальное время обнаружения отказа равно *Hello_Interval*. Для сокращения времени обнаружения отказа зачастую применяют средства

обнаружения канального или даже физического уровня. Данные способы будут рассмотрены ниже.

Время генерации и начала рассылки LSA-сообщения (*LSA_Generation_Time*). Если наступает событие, требующее генерации LSA-сообщения, то, первоначально, формирование этого сообщения будет задержано на временной интервал *Initial_Interval*. Когда это время истечет, LSA-сообщение будет сгенерированно, и запустится таймер хранения *Hold_Timer*. Любые события, связанные с изменением топологии сети в пределах интервала хранения *Hold_Timer*, не будут приводить к формированию нового LSA. Вместо этого эти события накапливаются, а единственное LSA-сообщение будет сгенерированно по окончании *Hold_Timer*. Таким образом таймеры *Initial_Interval* и *Hold_Timer* гарантируют, что если канал отказал и снова восстановился, то LSA сообщения, которые должны были сообщить смежным маршрутизаторам о пропадании канала, не будут отправлены, и процесс пересчета алгоритма SPF у других маршрутизаторов сети не будет запущен. Если после отправки LSA-сообщения о первоначальном изменении топологии в сети продолжаются изменения, то маршрутизатор будет увеличивать интервал хранения *Hold_Timer* по экспоненте [28, 30]:

$$Hold\_Timer = 2^{t \cdot Hold\_Timer},$$

пока он не достигает предварительного определенного значения *Max_Wait*. В этом случае время хранения *Hold_Timer* больше не будет увеличиваться и будет равно *Max_Wait* при любой динамике изменения топологии сети. В случае когда в течение интервала $2 \cdot Max\_Wait$ событий, приводящих к генерации LSA-сообщений не происходит, то таймер хранения *Hold_Timer* сбрасывается к своему начальному значению. Необходимо отметить, что интервал хранения должен примерно равняться (или немного превышать) полное время сходимости сети так, чтобы все маршрутизаторы успели отработать новые изменения топологии прежде, чем придет следующее LSA-сообщение [30].

Текущие значения интервалов распространяются по сети с помощью Hello-пакетов [33].

Таким образом, параметрами генерации и оправки LSA-сообщений являются [30]:

- *Initial_Interval* - время задержки перед отправкой LSA-сообщения;
- *Hold_Timer* - время, по истечении которого LSA-сообщение будет отправлено другим маршрутизаторам если других изменений топологии не произошло;
- *Max_Wait* – максимальное значение интервала ожидания *Hold_Timer*.

Оборудование Cisco по умолчанию использует значения *Initial_Interval*=10 мс, *Hold_Timer*=100 мс, *Max_Wait* =5000 мс.

Для контроля процесса лавинной рассылки сообщений LSA об обновлениях топологии в сетевом оборудовании (в IOS и в JunOS), в протоколах маршрутизации предусмотрены специальные временные параметры [30].

Смежным маршрутизаторам, как правило, отправляются два LSA сообщения с задержкой *Min_LS_Interval*. Так как лавинная рассылка LSA

должна является надежным процессом, то требуется подтверждения о приемах LSA-сообщений. В случае отсутствия таких подтверждений об успешном приеме, LSA-сообщения рассылаются снова после истечения таймера повторной передачи *Rxmt_Interval*.

Для протокола OSPF значениями по умолчанию являются: *Min_LS_Interval* =1 с, *Rxmt_Interval* =5 с [37].

Flood_packet-pacing_timer – устанавливает время задержки перед отправкой следующего LSA-сообщения после ранее отправленного.

Retransmission packet-pacing timer (*Rxmt_Interval*) – устанавливает время задержки перед повторной отправкой сообщения LSA, в случаях, если на ранее отправленное сообщение не пришло подтверждение об его успешном получении. В более усовершенствованной реализации данного таймера, предусмотренной RFC 4222 [34], реализован механизм повторной передачи за счет динамического изменения параметра *Min_LS_Interval.* В соответствии с RFC 4222 таймер *Rxmt_Interval* экспоненциально увеличивается каждый раз, когда число неподтвержденных сообщений LSA в очереди для повторной передачи превышает заданный порог (например, во время перегрузки сети). При успешном получении подтверждений о доставки LSA сообщений, интервал *Rxmt_Interval* снова сбрасывается к своему начальному значению.

Group packet-pacing timer. В протоколе OSPF ver. 2 для плановой коррекции таблиц маршрутизации предусмотрена массовая рассылка LSA сообщений каждые 30 мин. Такая рассылка сильно нагружает сеть, и в оборудовании Cisco предусмотрена задержка (по умолчанию 240 мс), на значение которой каждый из маршрутизаторов задерживает отправку своего LSA сообщение. Таким образом, формируется групповая рассылка, в которой сообщения LSA следуют с интервалом в 240 мс [35].

Время распространения LSA-сообщений о топологии всем маршрутизаторам в сети (*Event_Propagation_Time*). Время лавинного распространения информации о топологических изменениях в сети посредством пересылки LSA-сообщений может существенно варьироваться в зависимости от пропускной способности каналов связи. Таким образом, приблизительно время распространения можно оценить следующим образом:

- при учете средней связности сети:

$$T_{LSA} = \frac{\lambda_{LSA} D_{LSA} R\, S}{\sum_{i}^{N} C_i};$$

- без учета связности сети

$$T_{LSA} = \frac{\lambda_{LSA} D_{LSA} R}{\frac{1}{N}\sum_{i}^{N} C_i};$$

где: T_{LSA} – время распространения LSA-сообщений по сети [с]; λ_{LSA} – интенсивность отправки пакетов LSA [пак./с]; D_{LSA} – длина пакета LSA [бит]; R – средняя длина маршрута в сети, выраженная в количестве каналов связи; S – показатель связности узлов, определяемый средним числом каналов связи

смежных узлу; C_i – пропускная способность i-го канал связи в сети [бит/с]; N – количество каналов связи в сети.

Время распространения LSA-сообщений по сети в зависимости от различных факторов исследовалось в работах [36, 37].

Исследование, проведенное в работе [36], на сети, состоящей из 87 маршрутизаторов и 161 канала связи, показало следующий эффект. В случае если LSA-сообщения оправляются немедленно после обнаружения отказа, то время их распространения по сети определяется пропускной способностью каналов связи и составляет 0,01…0,05 с (рис. 1). Однако, если отправка LSA сообщений ведется в соответствии в вышеуказанными таймерами, то время достижения LSA сообщениями всех маршрутизаторов сети существенно зависит от временных параметров *Hello_Interval* и *Min_LS_Interval* (рис. 2).

Как показывает анализ результатов исследования [36], представленные на рис. 2, в подавляющем числе случаев (более 95%) при различных значениях временных параметров обнаружения отказа и рассылки LSA время достижения LSA сообщениями других маршрутизаторов сети практически совпадает со значением *Hello_Interval.*

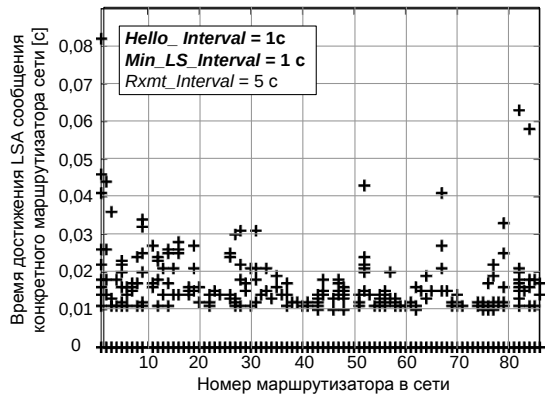
В работе [37] исследованы вопросы распространения LSA сообщений в сетях, построенных на основе низкоскоростных каналов. Показано, что в низкоскоростных каналах возникают перегрузки LSA сообщениями, приводящие к их потере, что, в свою очередь, приводит к лавинообразному нарастанию загрузки и, как следствие, к существенному росту времени сходимости в сети.

Время, необходимое для запуска алгоритма кратчайших путей после получения новых LSA-сообщений (*SPF_Run_Time*). Порядок запуска вычисления SPF определяется временными параметрами, которые предназначены для предотвращения частых вычислений SPF во время рассылок LSA сообщений, следующих с незначительным интервалом.

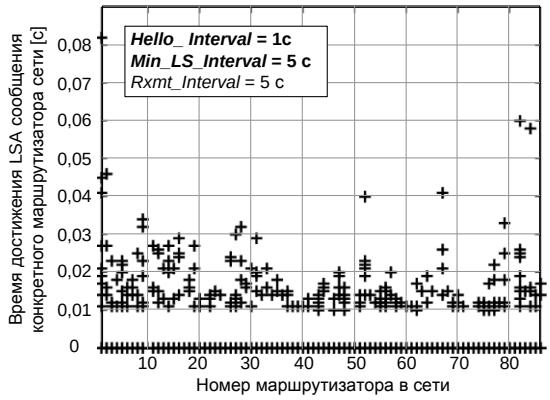
К данным параметрам относятся [30]:

- *SPF_Delay_Timer* - определяет время, которое маршрутизатор должен ожидать прежде чем выполнить вычисление SPF после получения первого LSA в расчете получить большее число LSA сообщений и произвести вычисление SPF с использованием последних данных об изменениях топологии сети;
- *SPF_Hold_Timer* - определяет задержку времени между двумя последовательными вычислениями SPF;

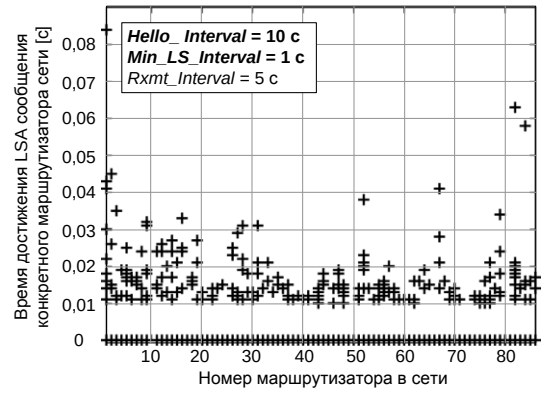
В сети, характеризующейся низкой интенсивностью отказов элементов, параметр *SPF_Hold_Timer* должен иметь малое значение, чтобы обеспечить быструю сходимость сети. В нестабильной сети, которой свойственны частые изменения топологии сети, маленькое значение *SPF_hold_Timer* может привести к частому вычислению алгоритма SPF. В таких сетях предпочтительно накапливать сообщения о нескольких топологических изменениях и обрабатывать их сразу. Для таких сетей рекомендуются большие значения параметров *SPF_Hold_Timer* и *SPF_Delay_Timer* [30].



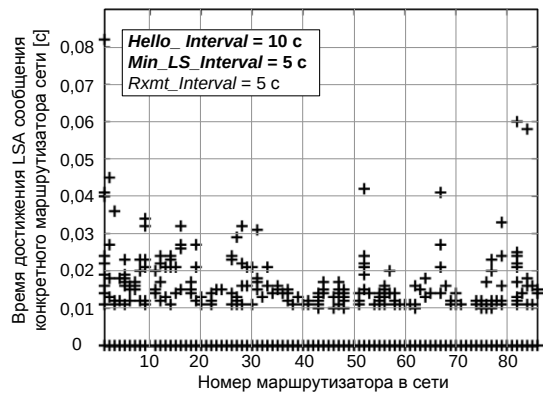
а.



б.

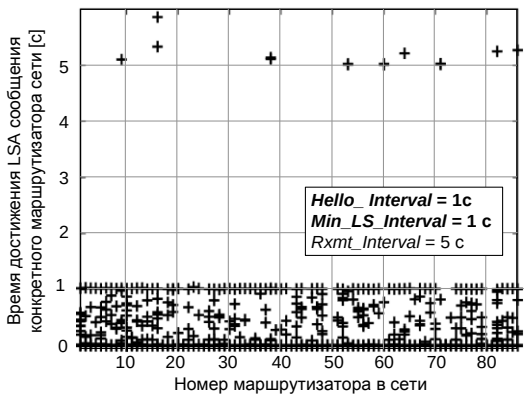


в.

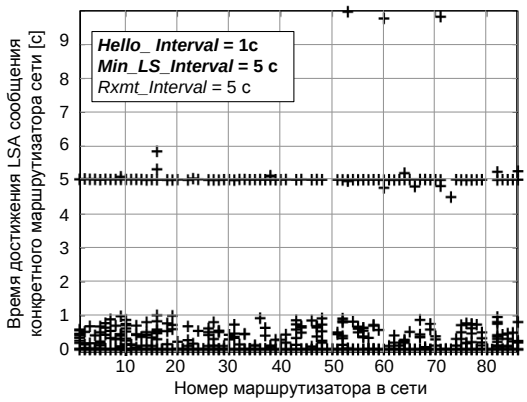


г.

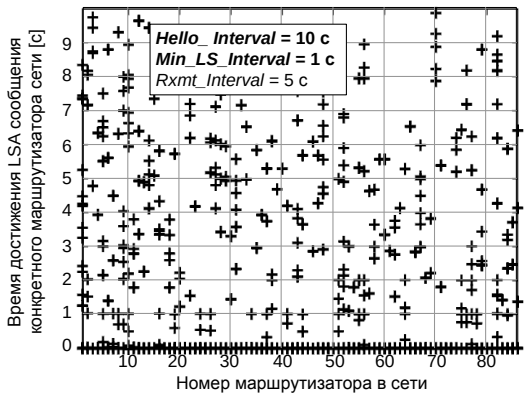
Рис. 1. Время достижения LSA сообщениями маршрутизаторов в сети без учета временных параметров обнаружения отказа и рассылки [36]



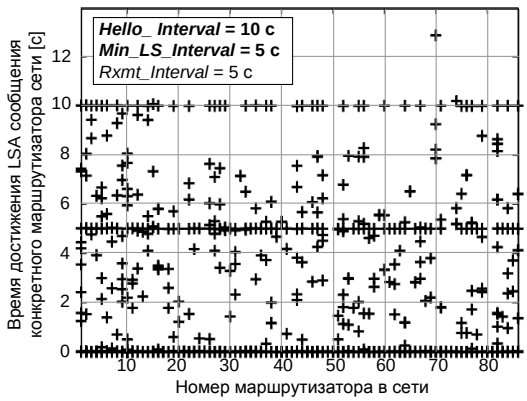
а.



б.



в.



г.

Рис. 2. Время достижения LSA сообщениями маршрутизаторов в сети с учетом временных параметров обнаружения отказа и рассылки [36]

Для протокола OSPF значениями по умолчанию являются: *SPF_Delay_Timer* = 5 с, *SPF_Hold_Timer*=10 с [37].

В современных маршрутизаторах (например, Cisco, после IOS 12.2 версии) процесс вычисления SPF, как правило, определяется тремя параметрами: *SPF_Start_Interval*, *SPF_Hold_Timer* и *SPF_Max_Wait*. Физический смысл этих параметров такой же, как и у аналогичных параметров отправки LSA сообщений [30].

- *SPF_Start_Interval* - время задержки перед выполнением SPF.
- *SPF_Hold* - определяет задержку времени между двумя последовательными вычислениями SPF. Данная задержка при выполнении каждого последующего вычисления SPF увеличивается по экспоненциальному закону [30]:

  $SPF\_Hold = 2^{t \cdot SPF\_Hold}$,

  пока не достигает предварительно определенного значения *SPF_Max_Wait*. В этом случае параметр *SPF_Hold* больше не будет увеличиваться и будет равен *SPF_Max_Wait* при любой динамике изменений топологии сети. Когда LSA-сообщения перестают приходить, и вычисления SPF больше не требуются, таймер *SPF_Hold* сбрасывается в свое начальное значение.

В оборудовании Cisco по умолчанию используются значения *SPF_Start*=10 мс, *SPF_Hold* =100 мс, *SPF_Max_Wait* =500 мс.

Время, необходимое для выполнения алгоритма SPF и обновления RIB/FIB таблиц маршрутизации (*RIB_FIB_Update_Time*). Вычислительная сложность алгоритма Дейкстры, который положен в основу SPF, равна $n\log(n)$ и в очень больших сетях может занять определенное время работы центрального процессора (ЦП) маршрутизатора. После успешного вычисления алгоритма поиска кратчайших путей SPF для тех путей, которые не совпадают с ранее вычисленными значениями, производится обновление таблиц RIB/FIB. Это является конечной целью процесса сходимости сети.

Длительность процесса вычисления алгоритма SPF исследовалась в работах [30, 38].

В работе [38] проведены экспериментальные измерения времени вычисления алгоритма SPF для сети со случайной топологией (моделировались высокопроизводительные платформы Cisco 7200 и Juniper M40). Результаты исследований представлены на рис. 3.

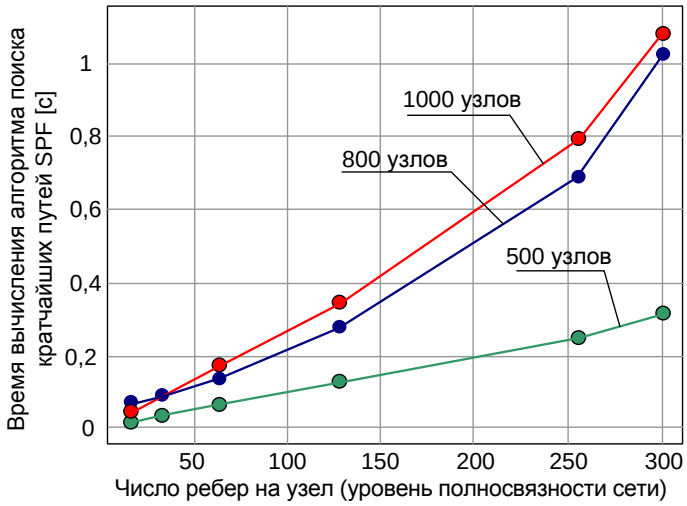


Рис. 3. Экспериментальные измерения времени вычисления SPF для сети со случайной топологией [38]

В работе [30] исследовалась загрузка маршрутизаторов при интенсивном периодическом отказе узла в сети, состоящей из 24 узлов и 49 каналов и использующей протокол OSPF (см. рис. 11). В данном исследовании показано, что даже при интенсивном отказе узла сети и необходимости постоянно пересчитывать SPF загрузка ЦП маршрутизатора не превышает 0,1%, что говорит о достаточности вычислительных возможностей современных маршрутизаторов.

Таким образом, время сходимости в сети зависит от множества параметров и может принимать довольно значительные значения (рис. 4), при этом основной вклад в длительность времени сходимости для конфигураций по умолчанию вносят временные параметры диагностики отказа, а также задержки в рассылке LSA сообщений и вычислении SPF.

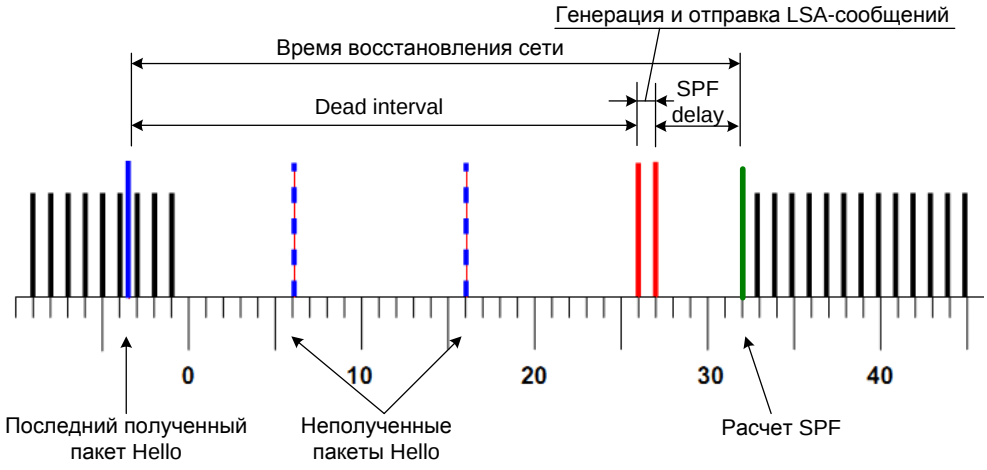


Рис. 4. Схема временных параметров, определяющих время сходимости сети

В таблице 2 приведены обозначения и значения основных временных параметров протокола маршрутизации OSPF, определяющие сходимость сети.

Таблица 2 - Значения временных параметров протокола маршрутизации определяющих сходимость сети для протокола OSPF [30, 37]

Параметры		Обозначение и значение
Временные параметры диагностики отказа	Период рассылки Hello-пакетов, для диагностики состояния смежности сети	*Hello_Interval* = 10 с (для обычной сети) 30 с (в широковещательной сети)
	Время ожидания восстановления связи после неполучения очередного Hello пакета. По истечении данного времени канал считается отказавшим, а смежный маршрутизатор - недоступным	*Dead_Interval*= 4×*Hello_Interval*
Временные параметры отправки сообщений об изменении топологии сети	Время задержки рассылки сообщения об изменении топологии сети	*Initial_Interval*=10 мс,
	Время, по истечении которого сообщение об изменении топологии будет отправлено другим узлам, если других изменений топологии не произошло	*Hold_Timer*=100 мс
	Максимальное время *Hold_Timer*	*Max_Wait* =5 с
	Период следования между двумя последовательно отправляемыми LSA сообщениями об изменении топологии	*Min_LS_Interval* =1 с
	Время после которого будет произведена повторная рассылка сообщения об изменении топологии, если получение предыдущего сообщения не подтверждено	*Rxmt_Interval* =5 с
Временные параметры вычисления алгоритма SPF	Задержка запуска алгоритма расчета кратчайших путей после получения очередного сообщения об изменении топологии	*SPF_Delay_Timer* = 5 с
	Время между двумя следующими подряд вычислениями алгоритма расчета кратчайших путей	*SPF_Hold_Timer*=10 с

На рис. 5 приведена схема, определяющая связь этих временных параметров с состояниями, в которых может находиться маршрутизатор, в соответствии с работой [39]. Такое представление позволяет наглядно оценить взаимосвязь временных параметров в процессе восстановления сети и их влияние на конечное время сходимости.

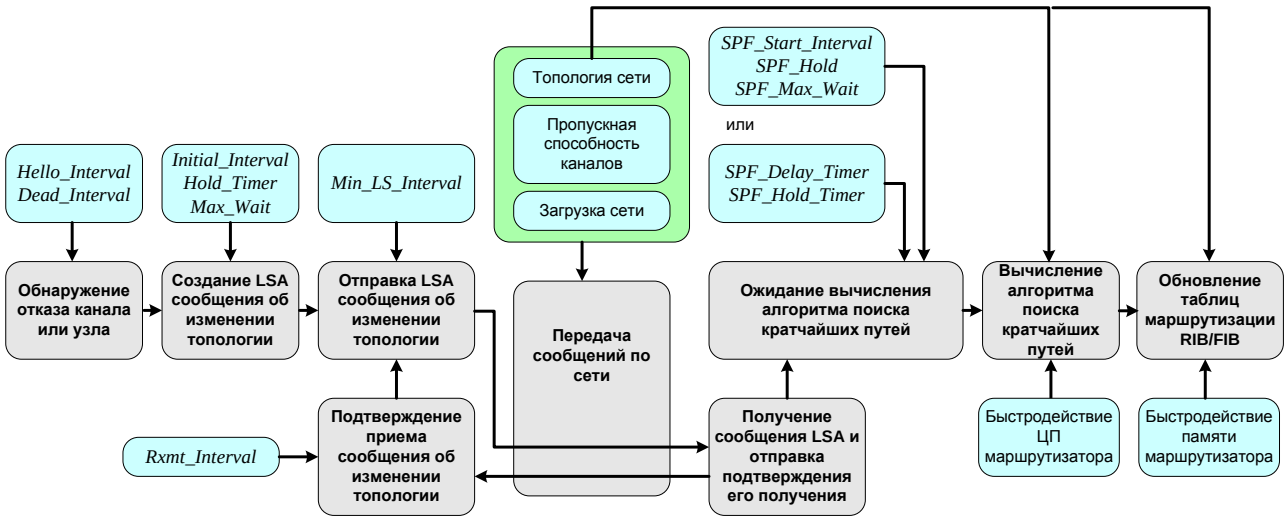


Рис. 5. Процесс сходимости сети OSPF [30, 39]

Временные таймеры, представленные на рис. 5, существенно влияют на устойчивость сети. В RFC 4222 [34] представлены рекомендации для администраторов, эксплуатирующих сети с протоколом OSPF v. 2, которые должны обеспечить высокую устойчивости сети и ее быструю сходимость.

- Необходимо присвоение высокого приоритета пакетам Hello и пакетам подтверждения состояния канала и низкого приоритета - остальным пакетам.
- Необходимо предусмотреть сброс таймеров отказа для канала после получения любых пакетов протокола маршрутизации по этому каналу вместо того, чтобы ожидать поступления очередного пакета Hello. Канал считать отказавшим не только в случае отсутствия пакетов Hello, но и в случае отсутствиях любых пакетов протокола маршрутизации за период *Router_Dead_Interval.*
- Для регулировки таймера оправки повторных пакетов LSA, при неподтверждении приема предыдущих (*Rxmt_Interval*), должен использоваться экспоненциальный алгоритм. Это позволит сократить количество повторных передач LSA-сообщений и предотвратить перегрузку низкоскоростных каналов сети.
- Для предотвращения перегрузки сети широковещательным служебным трафиком и повышения эффективности реакции протокола маршрутизации при частых отказах в сети целесообразно использовать алгоритмы экспоненциальной регулировки таймеров.
- Если конфигурация сети предусматривает случаи, когда большая группа маршрутизаторов будет включена/отключена в/из сети, то необходимо использовать задержку начала рассылки LSA-сообщений каждым из этих маршрутизаторов.

Однако выполнение даже этих рекомендаций не может обеспечить высокую устойчивость сетей, в связи с чем профильными комитетами и производителями телекоммуникационного оборудования предлагаются различные способы снижения времени сходимости сетей. Основные технологические подходы к таким способам представлены в следующем подразделе работы.

Основные технологические решения для протоколов маршрутизации направленные на снижение времени сходимости в сети

В работах [1, 30] рассмотрены основные варианты улучшений, применяемые в современных протоколах для повышения времени сходимости сети. При этом, в работе [30], в основном, приводится анализ улучшений, направленных на повышение устойчивости и снижение времени сходимости проводных сетей, а в работе [1] проведен анализ направлений модификации стандартных протоколов, основанных на оценке состояния каналов с целью их применения в мобильных радиосетях MANET.

Рассмотрим основные технологические решения, применяемые в протоколах маршрутизации и направленные на снижение времени их сходимости (рис. 6). При этом, основные направления развития данных

решений, на основе последних исследований, представлены в заключительной части статьи.

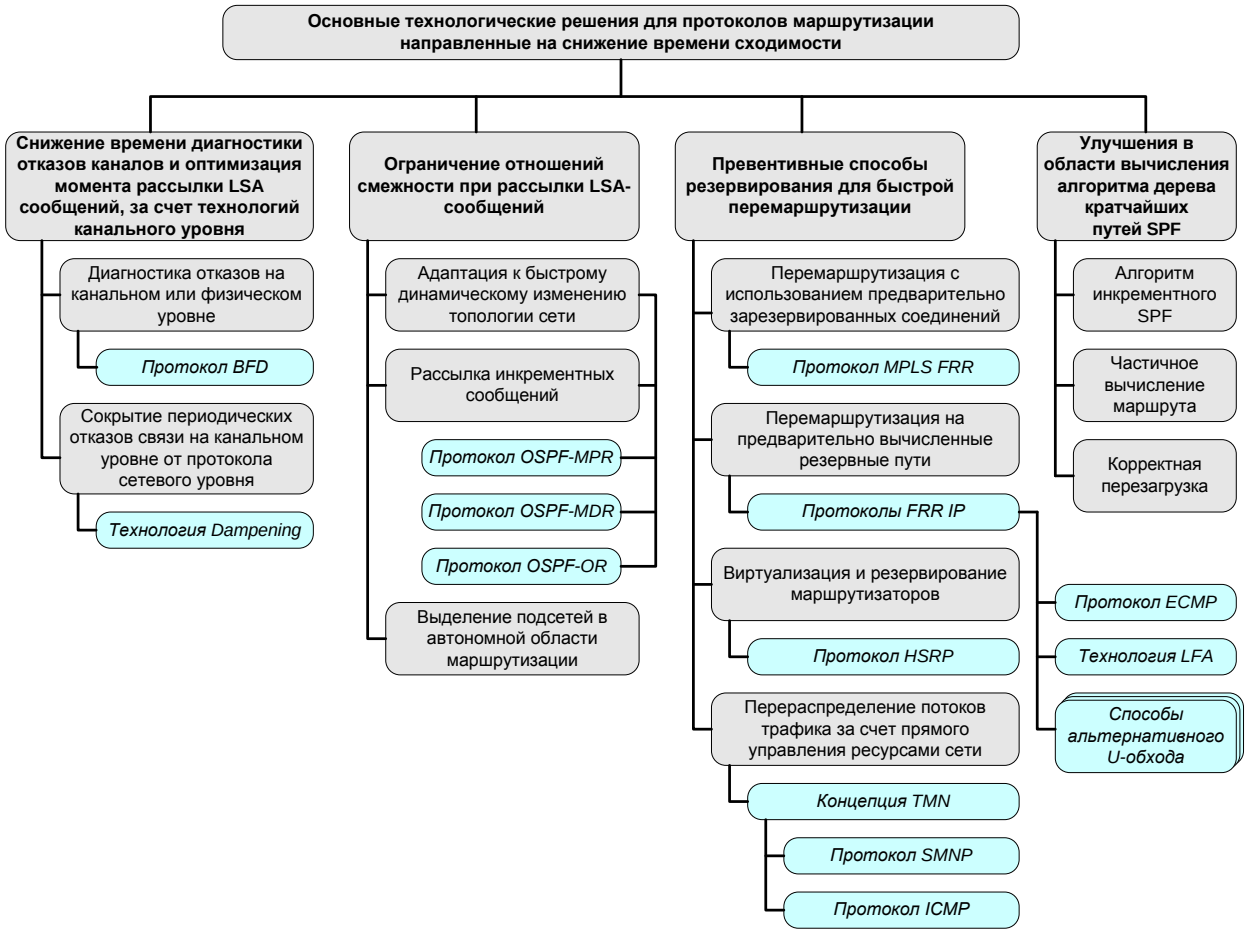


Рис. 6. Основные технологические решения, применяемые в протоколах маршрутизации для снижения времени сходимости

1) Снижение времени диагностики отказов каналов и оптимизация момента рассылки LSA сообщений, за счет технологий канального уровня.

1.1) Диагностика отказов на канальном или физическом уровне. Эффективным способом снижения задержек при диагностике отказов каналов связи является использование информации о состоянии каналов непосредственно от канального протокола или от каналообразующего оборудования. Одним из вариантов реализации такого способа является протокол BDF.

Протокол BFD (Bidirectional Forwarding Detection) [40] основан на милисекундных таймерах при двунаправленной проверке работоспособности пути, включая интерфейсы и каналы передачи данных между двумя маршрутизаторами [1, 30, 40, 41]. Протокол BFD реализован на канальном уровне модели OSI (Open Systems Interconnection) и предоставляет технологиям этого уровня, таким как Ethernet, сервис обнаружения отказа канала, сопоставимый по времени с технологиями транспортных сетей SONET/SDH (50 мс).

При использовании BDF смежные маршрутизаторы создают сеанс BFD и согласовывают время отправки и получения пакетов BFD с целью обнаружения

отказов в канале связи. Пакеты BFD встраиваются в информационный обмен канального уровня и, в случае потери очередного BDF-пакета, протокол диагностирует отказ канала, о чем он уведомляет маршрутизатор. Такой механизм позволяет маршрутизатору диагностировать отказ канала раньше, чем отказ будет обнаружен при использовании обмена Hello сообщениями.

1.2) Сокрытие периодических отказов связи на канальном уровне от протокола сетевого уровня. Данный способ предусматривает решение задачи диагностики отказов на канальном уровне и, в случае флуктуаций работоспособности канала, сокрытие этих изменений от сетевого уровня, чтобы последний не инициировал пересчет топологии. Одним из таких способов является технология Dampening, реализованная в операционной системе Cisco IOS (начиная с версии 12.0) и в BGP в junOS.

Технология Dampening [42, 43] предусматривает, что при каждом отказе канального интерфейса ему присваивается значение штрафа согласно формуле $P_n = 2^{-t/H} \cdot P_{n-1} + P_{n-1}$. В случае если это накопленное значение штрафа превышает допустимое пороговое значение, то интерфейс отключается. При снижении значения штрафа ниже порогового значения интерфейс включается и начинает снова использоваться.

Данный механизм использует пять параметров [30]:

1. *Штраф* (*либо другой показатель качества*). Первоначально – $P(0)=1000$. При отсутствии изменений топологии в каждый *Half_Life_Period* штраф экспоненциально снижается в соответствии с выражением:
   $$P(t)=P(0)\cdot 2^{-t/H}. \quad (1)$$
   Если счетчик топологических изменений больше единицы за время *Half_Life_Period*, штраф продолжает увеличиваться:
   $$2^{-t/H}\cdot P+P. \quad (2)$$
2. *Порог отключения* (*Suppress_Threshold*) - максимально накопленное значение штрафа, после которого канальный интерфейс отключается. Если счетчик штрафа больше единицы в *период полураспада*, штраф продолжает увеличиваться $2^{-t/H}\cdot P+P$. Значение порога отключения по умолчанию - *Suppress_Threshold*=2000.
3. *Время полужизни* (*Half_Life_Period*) - продолжительность времени, по истечении которого штраф по экспоненте снижается в соответствии с выражением (1). Это время выбирается на основе измерений флуктуаций канального интерфейса. Если счетчик отказов канального интерфейса больше 1 за время *Half_Life_Period*, штраф увеличивается в соответствии с выражением (2).
4. *Порог повторного использования* (*Reuses_Threshold*) – накопленное значение штрафа, после которого канальный интерфейс включается снова и начинает использоваться. Значение по умолчанию – 1000.
5. *Максимальное время подавления* (*Max_Suppress_Time*) – максимальное время, в течение которого канальный интерфейс может быть отключен. В случае если за данное время восстановление связи не произошло, то данный канал считается полностью отказавшим и маршрутизатор

переходит на использование альтернативного пути. Значение по умолчанию *Max_Suppress_Time*=4·*Half_Life_Period*.

Технология Dampening фактически дублирует функционал отложенной рассылки LSA-сообщений, и поэтому в маршрутизаторах эти два режима совместно не используются [30].

2) Ограничение отношений смежности при рассылке LSA-сообщений.

2.1) Установление отношений смежности только через основной и резервный маршрутизаторы сети. После запуска маршрутизатор, работающий на основе протокола по состоянию каналов в широковещательной сети, устанавливает наличие отношений смежности с другими маршрутизаторами за счет обмена Hello-ссообщениями. Однако в широковещательной сети (например, в радиосети со случайным множественным доступом), за счет лавинной рассылки сообщений любой другой маршрутизатор может считаться непосредственно-смежным соседом. Высокий уровень смежности ведет к усложнению топологии сети и приближению ее к полносвязной, что приводит к росту времени вычисления алгоритма SPF при изменениях в ней. Чтобы этого избежать в широковещательной сети маршрутизаторы, использующие протокол OSPF, выбирают основной маршрутизатор, называемый выделенным маршрутизатором (DR - Designated Router), и резервный выделенный маршрутизатор (BDR - Backup Designated Router). Маршрутизаторы DR и BDR устанавливают полную смежность со всеми маршрутизаторами в сети, а остальные маршрутизаторы устанавливают отношения смежности только с DR и BDR. В результате количество отношений смежности в сети значительно сокращается. Маршрутизатор DR рассылает широковещательные сетевые LSA-сообщения, перечисляющие все маршрутизаторы в сети. На основе этих LSA-сообщений от DR остальные маршрутизаторы корректируют свои таблицы маршрутизации [1].

2.2) Адаптация к быстрому динамическому изменению топологии сети. В мобильных сетях MANET отдельные маршрутизаторы могут динамически присоединяться или оставлять сеть, что заставляет протокол маршрутизации инициировать выдачу с высокой интенсивностью LSA-сообщений об изменении топологии сети. Инженерная группа IETF разработала несколько расширений для протокола OSPF в интересах обеспечения его эффективной работы в сетях MANET [1]:

- OSPF-MPR [44]
- OSPF-OR [45],
- OSPF-MDR [46].

Общим для различных расширений OSPF, используемых в MANET, является то, что они адаптируют протокол состояния связей для характеристик беспроводных сетей и используют альтернативные механизмы для уменьшения издержек и ускорения сходимости сети.

Протокол OSPF-MPR использует технологию многоточечной передачи MPR (Multi-Point Relaying). Каждый маршрутизатор выбирает из смежных ему маршрутизаторов те, через которые достижимы другие маршрутизаторы сети, и

помещает их в группу MPR (рис. 7). Таким образом, каждый маршрутизатор поддерживает отношения связности только с теми узлами, которые входят в его группу MPR, и с теми соседями, которые выбрали его в их собственный MPR. Это позволяет существенно уменьшить общее количество установлений смежности, необходимых в MANET. Чтобы предотвратить исключительный случай, когда сформированная группа MPR не охватывает всей сети, один из маршрутизаторов сети, называемый *синхронизирующим маршрутизатором,* устанавливает отношения смежности со всеми остальными маршрутизаторами [1].

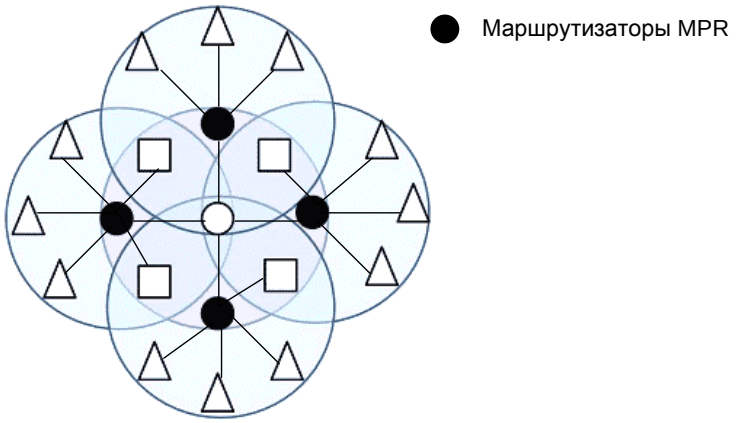


Рис. 7. Многоточечная передача по OSPF-MPR [1]

Протокол OSPF-OR основан на принципе недопустимости установления отношения смежности двумя маршрутизаторами в том случае, если они могут достигнуть друг друга в дереве кратчайшего пути SPT. В OSPF-OR, когда маршрутизатор получает Hello сообщение от нового маршрутизатора, он анализирует дерево кратчайших путей SPT для поиска совместного маршрутизатора-соседа. В случае если новый маршрутизатор достижим через другой маршрутизатор, уже имеющийся в дереве SPT, то отношение смежности с новым маршрутизатором устанавливается через него, без дополнительного обмена LSA-сообщениями. Если ни один из маршрутизаторов не является соседом нового, то это означает, что соседних маршрутизаторов в SPT нет, и требуется установка нового отношения смежности через обмен LSA. Если маршрутизаторы далее приходят к заключению, что принадлежат двум, до настоящего времени несвязанным, частям сети, то эти два маршрутизатора объединяют свои связующие деревья SPT в одно, за счет учета канала связи между этими двумя маршрутизаторами. Остальные маршрутизаторы в сети оповещаются о новом связующем дереве за счет широковещательной рассылки по каналам, входящим в дерево SPT. Данный подход аналогичен действиям протоколов маршрутизации по вектору состояний. При этом полноценный обмен LSA-сообщениями и полный пересчет связующего дерева SPT в OSPF-OR будет инициирован только при отказе канала связи, входящего в отношение смежности в текущем связующем дереве [1].

Протокол OSPF-MDR основан на снижении отношений связности за счет формирования соединенной магистрали выделенных маршрутизаторов DR,

называемых *выделенными маршрутизаторами MANET* (MDR - MANET Designated Router). Каждый маршрутизатор в сети является или MDR, или соседом MDR. Подобно стандартному протоколу OSPF, маршрутизаторы также формируют и резервную магистраль, состоящую из *резервных MDR* (BMDR). При этом, также по аналогии с OSPF, каждый маршрутизатор в сети является или BMDR, или соседом BMDR. Маршрутизаторы, включаемые в сеть, устанавливают отношения смежности только с MDR и BMDR, а через них и с другими маршрутизаторами сети [1].

2.3) Рассылка инкрементных сообщений. Для сокращения объема служебной информации вышеуказанные расширения OSPF для MANET используют следующие механизмы устранения избыточности [1]:

- инкрементные сообщения Hello [45];
- дифференциальные сообщения Hello [46].

Механизм инкрементных сообщений Hello в составе протоколов OSPF-MPR, OSPF-OR и OSPF-MDR позволяет маршрутизаторам сообщать только об изменениях, произошедших в их окружении в течение длительности последнего *Hello_Interval*, вместо полной информации об окружении. Таким образом, если сеть будет устойчива, то большинство сообщений Hello будет иметь значительно меньший объем. Однако при использовании этих механизмов отказы каналов или изменения топологии могут вызвать потерю Hello-синхронизма, так как не позволят узлам сети отслеживать изменения топологии должным образом. Чтобы обнаружить эти случаи вводится нумерация пакетов Hello и контроль правильной последовательности их приема.

Дифференциальные сообщения Hello используют превентивный механизм восстановления синхронизма, в то время как инкрементные сообщения Hello делают их получателя ответственным за управление синхронизацией. Эти механизмы, используемые совместно, позволяют отследить изменение топологии, а также снизить объем служебного трафика в MANET сети.

Аналогичные подходы могут применяться и для рассылки LSA сообщений при изменении топологии сети.

2.4) Выделение подсетей в автономной области маршрутизации. Протоколы внутридоменной маршрутизации могут предусматривать декомпозицию одной большой области маршрутизации на несколько небольших подсетей. Это позволяет уменьшить размер хранимых таблиц маршрутизации и ограничить область рассылки LSA-сообщений отдельной подсетью в случае отказа канала [1, 50].

3) Улучшения в области вычисления алгоритма дерева кратчайших путей SPF. Алгоритм SPF, как правило, использует алгоритм Дейкстры для вычисления путей к узлам сети. Одним из его недостатков является необходимость полного пересчета путей для таблиц маршрутизации при получении сообщения LSA об изменении топологии сети. Вместе с тем, при изменении топологии в дереве путей могут быть части, которые останутся неизменными, и их пересчет не нужен.

3.1) Алгоритм инкрементного SPF. Алгоритм инкрементного SPF (iSPF - Incremental SPF) является более новой версией SPF, которая позволяет избежать ненужных вычислений за счет анализа информации в LSA сообщениях и сопоставления ее с уже построенным в протоколе деревом кратчайших путей SPT. Алгоритм iSPF, получая новый LSA, вычисляет SPF по алгоритму Дейкстры и при этом дополнительно учитывает следующие правила [30].

- Если изменением топологии является добавление нового конечного узла, то дерево путей наращивается до этого узла без полного пересчета;
- Если в результате изменения топологии произошел разрыв путей до конкретных узлов, то iSPF будет инициирован для пересчета путей только от корня до этих узлов, пути к которым были проложены через отказавший канал. Для пересылки данных до узлов, пути которых не изменились, будет использовано дерево, рассчитанное ранее.
- Если в сети появляется новый канал между узлами, к которым уже проложены пути, то пересчет дерева путей не производится.

Алгоритм iSPF является более эффективным для сетевых топологий с меньшей плотностью соединений. При этом, чем более отдаленным от текущего узла является отказ, тем менее трудоемким будет выполнение алгоритма iSPF.

3.2) Частичное вычисление маршрута. Алгоритм частичного вычисления маршрута PRC (Partial Route Computation) используется в протоколе IS-IS и OSPF v.3 и основан на следующем принципе. Каждый раз, когда через маршрутизатор проходит пакет с IP-адресом, содержащим новую сеть, маршрутизатор добавляет эту сеть в таблицу маршрутизации, а дерево путей продляется до этой сети через тот узел, от которого этот пакет был получен. Таким образом не инициируется полный пересчет дерева кратчайших путей, а только наращивается уже рассчитанное древо.

В OSPF v.3 дополнительно к LSA сообщениям с IP адресами используются LSA сообщения, в которых идентификаторы LSA, такие как идентификатор маршрутизатора, идентификатор области маршрутизации и метрика состояния канала, которые являются 32 битными числами. Эти числа однозначно определяют каждый маршрутизатор в области маршрутизации в отличие от OSPF v. 2, который идентифицирует смежные маршрутизаторы по их IP-адресам. Таким образом, в OSPF v.3 информация о доступности IP сетей полностью отделена от информации о доступности маршрутизаторов. В результате, LSA сообщения типов 1 и 2 генерируются и передаются только если изменилась топология и требуется инициализация алгоритма SPF для пересчета путей. При этом LSA сообщения о доступности/недоступности отдельных IP сетей генерируются и передаются при обнаружении/отключении отдельной IP сети и ведут только к изменению информации о префиксах IP, не инициируя пересчет дерева кратчайших путей [1, 51].

3.3) Корректная перезагрузка. Функция корректной перезагрузки поддерживается оборудованием Cisco IOS и JunOS и предусмотрена в RFC 3623 [1, 30, 52]. Данная функция позволяет в случае необходимости проведения

регламентных работ обеспечить корректное временное выведение маршрутизатора из работы в сети без инициализации пересчета топологии. Для реализации корректной перезагрузки используется современное логическое разделение архитектуры области маршрутизации на плоскость управления и плоскость данных.

Маршрутизатор, который планируется к перезагрузке, непосредственно перед ней сохраняет свое состояние в энергонезависимой памяти для последующего восстановления в том же состоянии после перезагрузки и отправляет своим смежным маршрутизаторам специальное локальное LSA сообщение, называемое *grace LSA.* Сообщение *grace LSA* не пересылается получившими его маршрутизаторами далее по сети, оно уведомляет о том, что отправивший его маршрутизатор корректно выйдет из сети на время перезагрузки. Таким образом, изоляция временной неработоспособности конкретного маршрутизатора только в зоне его смежных узлов позволяет не начинать процесс пересчета SPF в сети. При этом маршрутизаторы, получившие сообщение *grace LSA*, продолжают работать так, как будто перегружаемый маршрутизатор доступен, однако временно приостанавливают отправку данных в его адрес.

Большинство реализаций функции корректной перезагрузки предусматривают, что после успешной перезагрузки маршрутизатор повторно инициирует себя в сети путем рассылки стандартных LSA сообщений. С одной стороны, это позволяет избежать топологических несоответствий, если в сети за время перезагрузки изменилась топология. С другой стороны, это практически сводит на нет основные преимущества данного способа, так как после такой лавинной рассылки LSA будут повторно запущены алгоритмы расчета SPF и на других маршрутизаторах.

Производители сетевого оборудования не рекомендуют использовать функцию корректной перезагрузки при наличии в сети отказов каналов и, как правило, эта опция обычно отключается в конфигурациях по умолчанию [1, 30].

4) Превентивные способы резервирования для быстрой перемаршрутизации. Вышерассмотренные способы повышения сходимости сети являются реактивными, то есть новые маршруты определяются только после того, как отказ произошел. Превентивные способы предусматривают, что новые маршруты вычисляются заранее, что позволяет избежать дополнительных временных затрат на оповещение соседних узлов и вычисление алгоритма SPF. Это позволяет превентивным способам обеспечить восстановление связи, сравнимое с восстановлением в транспортных сетях (50 мс).

Подробный анализ превентивных способов восстановления сети после отказа представлен в работах [1, 47]. Как правило, данные способы используют предварительное резервирование сетевых ресурсов и являются частью отдельных технологий управления трафиком, используемых в транспортных сетях.

4.1) Перемаршрутизация с использованием предварительно зарезервированных соединений. Данный способ применяется в транспортных сетях на основе протоколов маршрутизации с установлением соединений (как правило, на основе PNNI и MPLS) и состоит в выделении части общего пула виртуальных соединений в резерв, который в дальнейшем используется при отказе основных соединений.

Примером реализации данного способа, функционирующего в MPLS сетях, является *протокол MPLS FRR* (Multi-Protocol Label Switching Fast Reroute) [48, 49]. Многопротокольная коммутация по меткам MPLS является технологией быстрой передачи пакетов с установлением соединения, и согласно модели OSI, находится между канальным и сетевым уровнями. Технология MPLS не заменяет IP маршрутизацию, но может предоставить дополнительные услуги по управлению трафиком (TE - Traffic Engineering), которые, в том числе, включают в себя и балансировку трафика через различные каналы в сети и быструю перемаршрутизацию на резервные пути. Расширение OSPF-TE, представленное в RFC 4203 [55], ориентированно на обеспечение и поддержание служб MPLS за счет управления маршрутизацией трафика сообщений по путям LSP (Label Switched Paths) в составе сети. Протокол MPLS FRR основан на использовании резервных путей LSP чтобы защитить основные LSP в случае отказов и базируется на протоколе резервирования сетевых ресурсов RSVP-TE [56]. MPLS FRR реализует локальный механизм защиты, когда узел, являющийся смежным к отказавшему элементу сети, переключает трафик с основных LSP на резервные. Резервные LSP позволяют трафику обходить отказавший элемент и восстановиться с основным LSP в узле слияния. Для резервирования LSP применяются схемы резервирования, стандартные для транспортных сетей: 1+1, 1:1, 1:*n* и *m*:*n* [1].

Основной сложностью быстрой перемаршрутизации при предварительном резервировании путей является то, что резервирование ресурсов сети происходит на начальном этапе установления соединений. Таким образом, подобное решение неприемлемо для чистых IP сетей, использующих адаптивно-лавинные протоколы маршрутизации без установления соединений.

4.2) Перемаршрутизация на предварительно вычисленные резервные пути. Особенностью IP сетей является то, что в них предварительные соединения не устанавливаются, и каждый маршрутизатор самостоятельно принимает решение о пути поступающих к нему пакетов. Поэтому в этих сетях каждый маршрутизатор предварительно вычисляет пути (как правило, на этапе вычисления SPT), по которым будет передаваться трафик в случае отказов.

Множество способов быстрой перемаршрутизации в IP сетях объединяются понятием FRR IP (FRR - Fast Reroute). Способы FRR IP подобны протоколу MPLS FRR в том смысле, что они оба используют заранее вычисленные резервные маршруты, которые позволяют обойти отказ элемента сети без необходимости сразу же сообщать другим маршрутизаторам об отказе. Однако отличие способов FRR IP от MPLS FRR состоит в том, что каждый маршрутизатор предварительно вычисляет резервные пути, которые будут им использоваться при локальном отказе в сети. Если у маршрутизатора имеются

несколько путей равной метрики до узла назначения и некоторые из них не проходят через отказавшие элементы сети, то такие пути используются в качестве путей восстановления в соответствии с протоколом ECMP. В отсутствие таких путей маршрутизатор ищет другие резервные пути, которые будут иметь худший показатель метрики, но они не проходят через отказавший элемент сети.

Рассмотрим несколько базовых решений, применяемых для обеспечения быстрого восстановления связи.

Протокол ECMP (Equal Cost Multi-Path) позволяет в составе одного маршрута использовать несколько путей равной стоимости. Если на этапе вычисления кратчайших путей было обнаружено несколько путей с равной метрикой между одной парой абонентов, то ECMP позволяет их использовать, поочередно выбирая каждый из них с равной вероятностью (алгоритм Round-robin). Каждые 10 минут таблица маршрутизации обновляется. Маршруты в ECMP проходить как между двумя смежными маршрутизаторами, так и через несколько маршрутизаторов в сети. В общем случае протокол ECMP применяется для балансировки нагрузки на сеть, однако он обеспечивает и надежность маршрутизации при отказах. Так, при отказе одного из путей происходит переключение на стандартную однопутевую схему, при этом рассылка LSA сообщений и пересчет топологии ведется уже после такого переключения. Схема совместного использования OSPF и ECMP реализована в протоке OSPF-ECMP [1].

Технология LFA (Loop Free Alternate) предложена для IP сетей в RFC 5286 [57] и основана на поиске циклов, проходящих через маршрутизатор- источник и другие маршрутизаторы в сети. При отказе канала связи протокол маршрутизации в качестве резервного пути использует части предварительно рассчитанного цикла, в который входит маршрутизатор-источник и маршрутизатор, недоступный в результате отказа [1].

Способы альтернативного U-обхода. Если пути ECMP/LFA не доступны, маршрутизатор может сформировать обходной путь за счет отправки трафика в направлении источника, но через другой маршрутизатор у которого в таблице маршрутизации может храниться альтернативный путь к узлу назначения. Пути восстановления через такие маршрутизаторы называют путями восстановления мультитранзитного участка, и стандартный способ такого восстановления представлен в RFC 5714 [58].

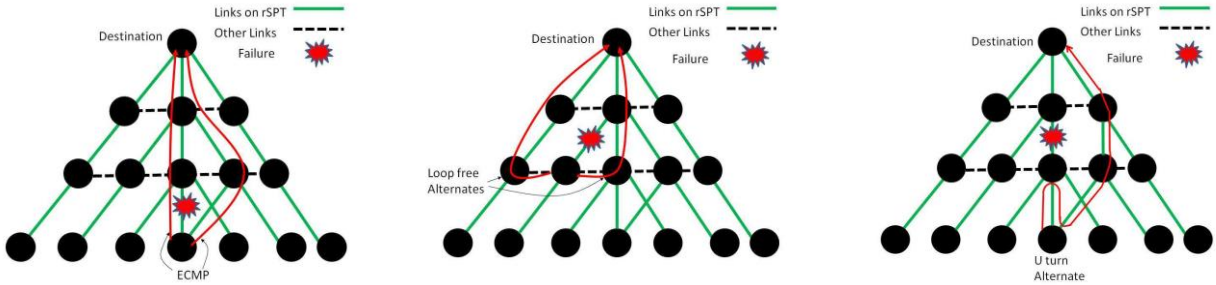
В настоящее время предложено несколько вариантов реализации способов альтернативного U-обхода [1]:

- прямое указание в заголовке IP пакета на запрет пересылки пакета маршрутизатору, у которого отказал канал [59];
- отправка пакета другому маршрутизатору, который имеет альтернативные отношения связности с областью, в которой находится узел-получатель [60];
- использование маршрутизаторами нескольких топологических конфигураций SPT (мультитопологий) с возможностью перехода

между ними в случае отказа канала, используемого в текущем SPT [61];

- тунелирование трафика в направлении U-обхода отказавшего элемента к месту, где может быть продолжена его нормальная передача, при этом в качестве механизмов тунелирования могут быть использованы IP в IP по RFC 1853 [62] или GRE по RFC 1701 [63].

Примеры использования различных вышерассмотренных способов перемаршрутизации на предварительно вычисленные резервные пути приведены на рис. 8.



а. Протокол ECMP б. Технология LFA в. Способ альтернативного U-обхода

Рис. 8. Примеры использования различных способов перемаршрутизации на предварительно вычисленные резервные пути [1]

4.3) Виртуализация и резервирование маршрутизаторов. Современные технологические решения позволяют объединить группу маршрутизаторов в единый виртуальный маршрутизатор. При этом внутри этой группы предусмотреть механизмы резервирования, балансировки нагрузки, расширения производительности, отказоустойчивости и т.д. Примером реализации такой виртуализации является протокол HSRP (Hot Standby Router Protocol), описываемый в RFC 2281 [53].

4.4) Перераспределение потоков трафика за счет прямого управления ресурсами сети. Policy Routing - политика маршрутизации, которая позволяет создавать отдельные правила и таблицы маршрутизации для различных типов трафика. Внутри этих правил может быть предусмотрены как дополнительные настройки балансировки нагрузки, так и различные сценарии маршрутизации при отказах в сети. Кроме того, для управления маршрутизацией может быть использована реконфигурация протоколов маршрутизации на основе протоколов управления сетевыми ресурсами TMN, SMNP и ICMP [54].

Помимо вышеперечисленных сетевых способов повышения устойчивости сети и снижения ее времени сходимости дополнительно могут быть использованы технологии и протоколы, находящиеся выше сетевого уровня модели OSI. Анализ использования таких технологий для восстановления сети после отказа ее элементов приведен в работе [64].

Анализ результатов исследований по оценке времени сходимости сети

При разработке новых способов снижения времени сходимости, как правило, требуется проведение оценки данного времени для стандартных реализаций протоколов маршрутизации и его сравнительный анализ с предлагаемыми модификациями. В этой связи, ниже приводится краткий обзор работ по исследованию времени сходимости в сетях. При этом отметим, что подавляющее число такого рода исследований выполнено на основе моделирования протоколов маршрутизации в программной среде OPNET.

В работе [65] представлены исследования времени сходимости сети для протоколов RIP, OSPF на основе моделирования в среде OPNET. Топология исследуемой сети представлена на рис. 9. В сети было образовано две виртуальных подсети DS1 и DS3. Исследовалось время сходимости сети в зависимости от временных параметров отказов канала связи между R1 и R2. Авторы использовали настройки протоколов OSPF и RIP по умолчанию. Результаты исследования приведены на рис. 10.

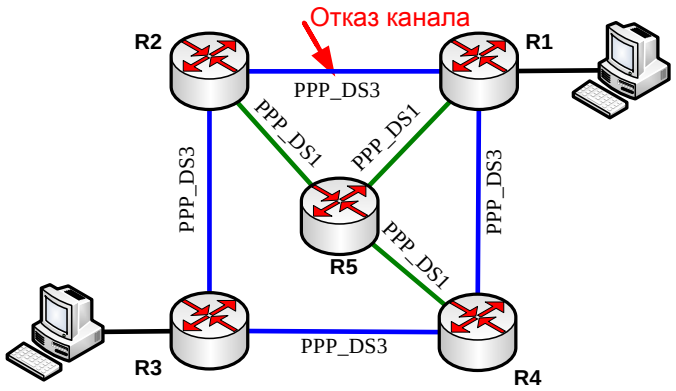
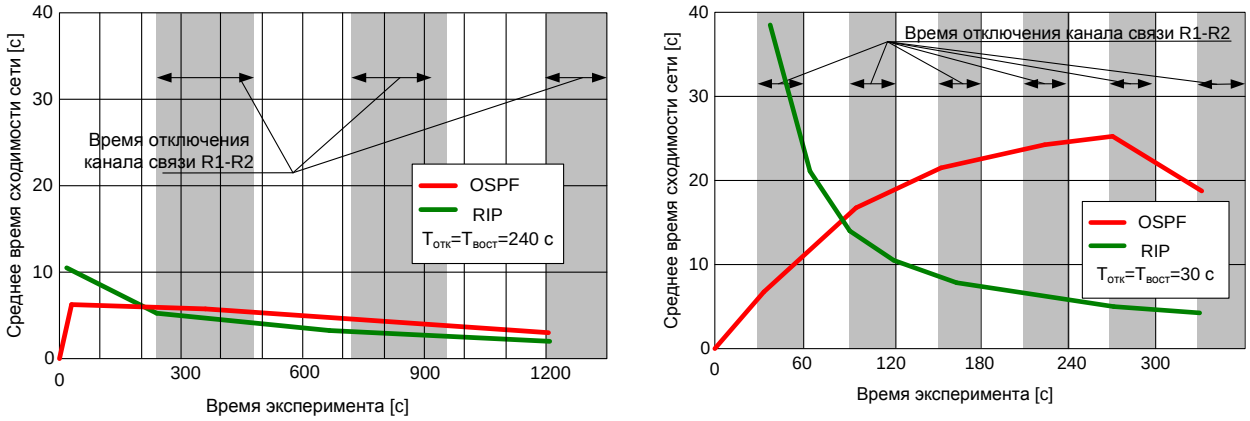


Рис. 9. Топология исследуемой сети на основе моделирования сети на основе маршрутизаторов Cisco 7200 в работе [65]



а. б.

Рис. 10. Результаты моделирования времени сходимости сети в OPNET, представленные в работе [65]

Как отмечается авторами работы [65], более высокая частота отказов канала R1-R2 ведет к повышению времени сходимости сети. К дискуссионным вопросам, отмечаемым авторами работы, относится более высокая

эффективность протокола RIP над протоколом OSPF, по критерию минимизации времени сходимости сети, что расходится с общепринятым мнением об эффективности данных протоколов. Для объяснения более быстрой сходимости протокола RIP авторы указывают на значение времени ожидания восстановления связи (dead time). У OSPF данный интервал равен 40 с, что в три раза меньше чем у RIP (180 с). Таким образом, OSPF инициирует реконфигурацию сети в три раза чаще по сравнению с RIP за один и тот же функциональный интервал и, следовательно, среднее время сходимости OSPF - больше.

Особый интерес представляют работы, в которых проводились как моделирование, так и экспериментальные исследования сходимости сети на реальном оборудовании, а также сравнение этих результатов.

В работе [30] в среде OPNET проведено исследование сети, использующей протокол OSPF состоящей из 24 узлов и 49 каналов, с топологией, представленной на рис. 11.

Сетевые компоненты на рис. 11: универсальные маршрутизаторы slip8_gtwy_690_upgrade, соединения – PPP SONET OC48 со скоростью передачи данных 2488,32 Мбит/с. В работе исследовалось время сходимости сети при различных значениях таймера Hello, таймера повторной передачи и таймеров задержки расчета алгоритма поиска кратчайших SPF, в частности:

1) влияние сокращение интервала Hello с 10 с до 1 с на скорость сходимости и загрузку центрального процессора (ЦП) маршрутизатора при однократном и многократном периодическом отказе узла сети;
2) влияние временных параметров задержки вычисления алгоритма SPF (*SPF_Delay_Timer* и *SPF_Hold_Timer*) на устойчивость сети и время сходимости.

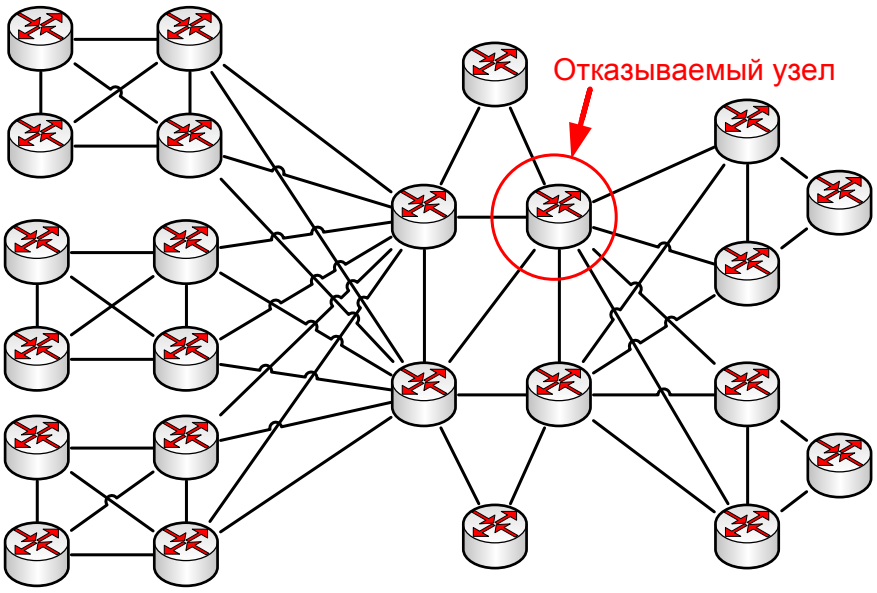


Рис. 11. Топология сети, исследуемая в работе [30]

Влияние сокращения интервала Hello с 10 с до 1 с на скорость сходимости и загрузку ЦП маршрутизатора при однократных отказах узла в сети представлено на рис. 12, 13.

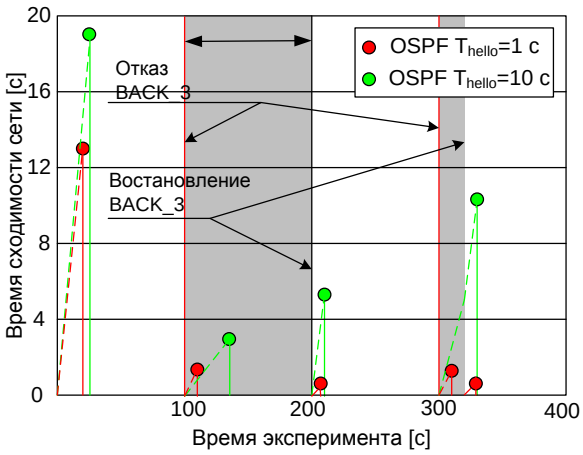


Рис. 12. Время сходимости сети при отказе/восстановлении узла [30]

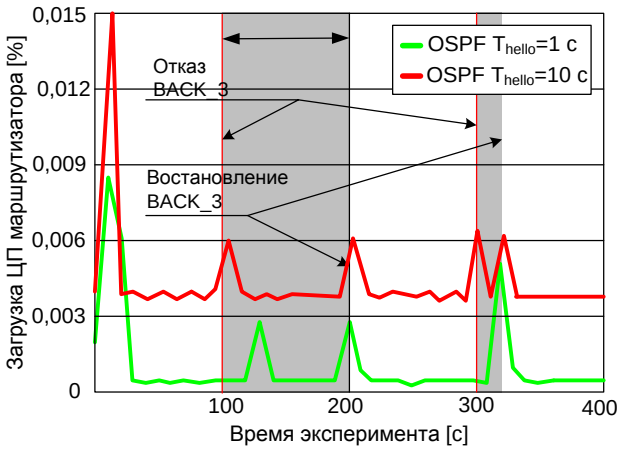


Рис. 13. Загрузка ЦП маршрутизатора при отказе/восстановлении узла [30]

Графические зависимости на рис. 12 показывают, что сокращение интервала рассылки Hello сообщений существенно снижает время сходимости сети из-за более быстрого обнаружения отказа и восстановления. Кроме того, снижение интервала Hello ведет к тому, что в ряде случаев алгоритм SPF инициализируется чаще. В частности, при *Hello_Interval*=1 с обновление таблицы маршрутизации в сети происходит дважды после отказа на 300 секунде функционирования сети (рис. 12). Это происходит из-за того, что уменьшение *Hello_Interval* приводит к пропорциональному уменьшению таймера ожидания восстановления связи *Dead_Interval*, в результате быстрее генерируются LSA сообщения, которые провоцируют пересчет SPF. Двойное вычисление SPF соответствует двойному пику нагрузки ЦП на рис. 13 в интервале 300-350 с времени моделирования.

Таким образом, снижение интервала Hello, несомненно, позволяет более быстро обнаружить отказ, но, в то же время, снижение данного параметра может стать причиной дополнительных циклов вычисления алгоритма SPF, что не лучшим образом скажется на общей стабильности сети и времени ее сходимости, в целом.

В работе [30] также было проведено моделирование влияния периодических (с интервалом 20 с) отказов/восстановлений узла сети на скорость сходимости и загрузку ЦП маршрутизатора при интервалах рассылки Hello 10 с и 1 с (рис. 11). Результаты моделирования представлены на рис. 14, 15.

Анализ графических зависимостей на рис. 14 позволяет подтвердить ранее сделанный вывод о том, что снижение интервала Hello позволяет более быстро обнаружить отказ, одновременно приводя к дополнительным циклам пересчета алгоритма SPF. При этом загрузка ЦП маршрутизатора возрастает вдвое, но остается в незначительных пределах (рис. 15).

Увеличение интервала Hello с 1 до 10 с эквивалентно «загрублению» реакции протокола маршрутизации на отказы в сети. При *Hello_Interval*=10 с (T_{hello}=0,5$T_{отк}$) сеть реагирует на каждое четвертое событие требующие пересчета топологии, в то время как при *Hello_Interval*=1 с (T_{hello}=0,1$T_{отк}$), каждый факт отказа или восстановления узла инициирует пересчет алгоритма SPF.

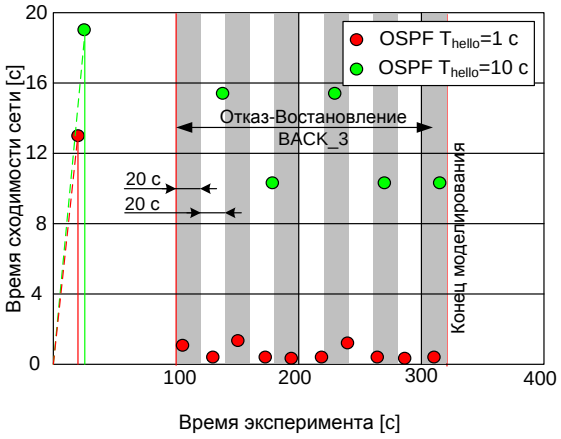


Рис. 14. Время сходимости сети при периодическом (20 с) отказе/восстановлении узла в сети [30]

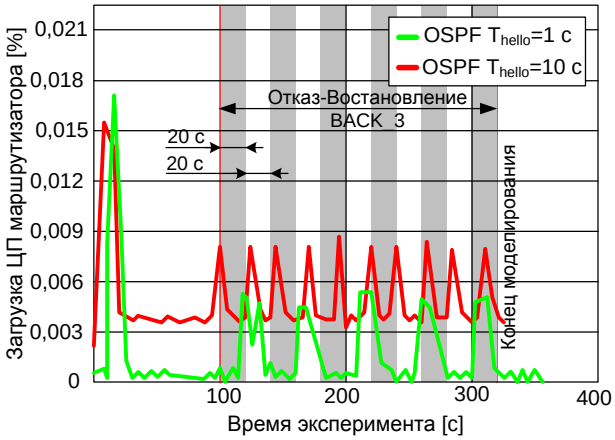
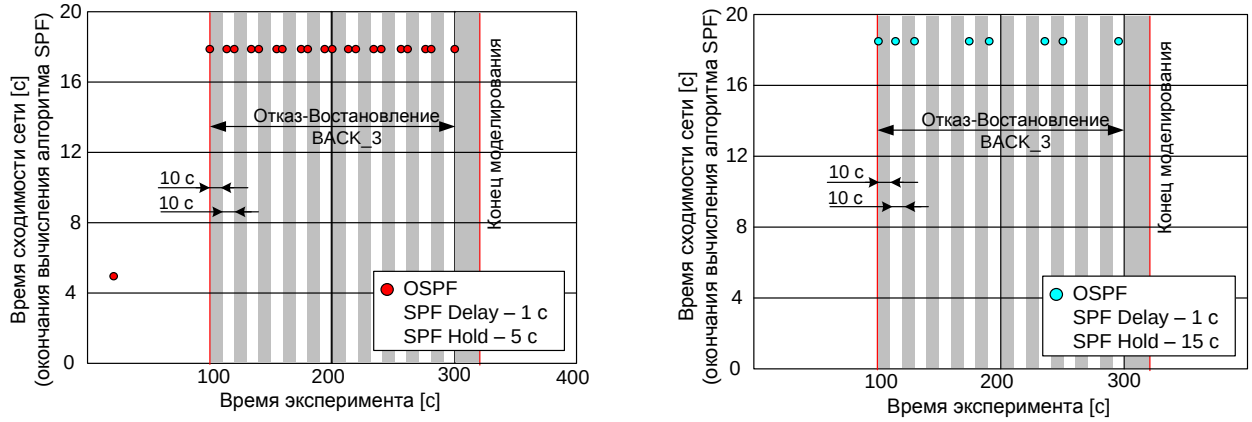


Рис. 15. Загрузка ЦП маршрутизатора при периодическом (20 с) отказе/восстановлении узла в сети [30]

Для дополнительного исследования влияния временных параметров запуска вычисления SPF в работе [30] было проведено моделирование периодических отказов/восстановлений узла сети (рис. 11) с интервалом 10 с при различных значениях интервала между двумя выполняемыми подряд вычислениями алгоритма SPF (*SPF_Hold_Timer*). Задержка выполнения алгоритма расчета кратчайших путей после получения очередного сообщения об изменении топологии в обоих эксперимента принималась равной *SPF_Delay_Timer* = 1 с. Время между двумя следующими подряд вычислениями алгоритма расчета кратчайших путей в различных экспериментах было равно: $SPF\_Hold\_Timer_1$=5 с и $SPF\_Hold\_Timer_2$=15 с. Результаты моделирования представлены на рис. 16.

Анализ результатов моделирования (рис. 16) показывает, что увеличение времени между двумя вычислениями алгоритма SPF (*SPF_Hold_Timer*) с 5 до 15 с приводит к уменьшению количества вычислений SPF примерно в 2 раза, при одном и том же значении времени сходимости сети. Это происходит из-за того, что за более длительный интервал *SPF_Hold_Timer* маршрутизаторы в сети успевают получить большее количество LSA сообщений об отказе узла и производят расчет SPF, ориентируясь на последнее из полученных сообщений.

Таким образом, с одной стороны увеличение времени между вычислениями алгоритма SPF позволяет снизить количество дополнительных пересчетов алгоритма SPF, а с другой - возрастает вероятность топологических несоответствий между реальным состоянием сети и топологией сети, указанной в таблице маршрутизации, которой руководствуется маршрутизатор при передаче трафика в сети.

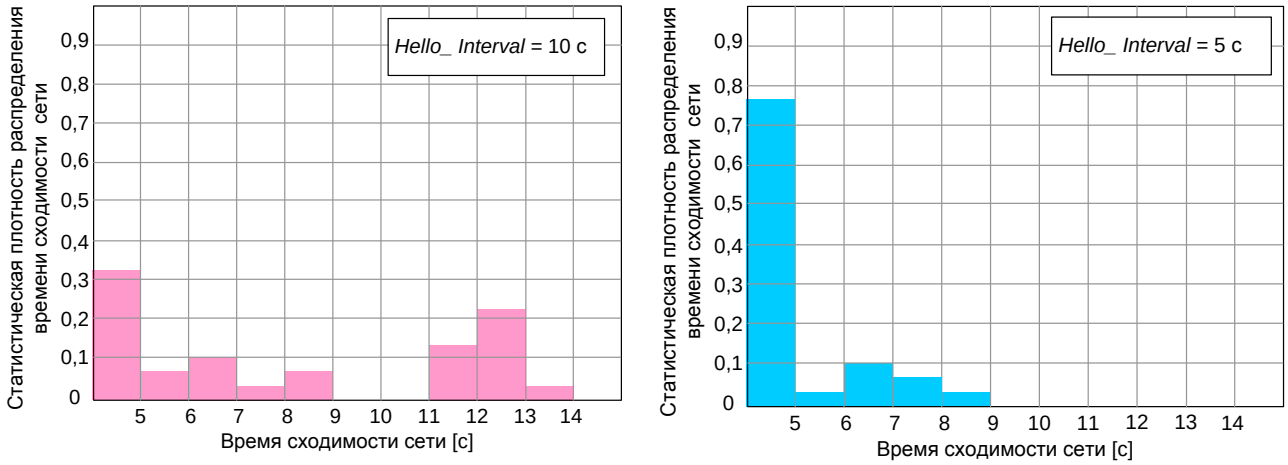


а. б.

Рис. 16. Исследование влияния временных параметров запуска алгоритма SPF на количество и время сходимости сети [30]

Вышеизложенные эффекты от воздействия периодических отказов элементов сети подтверждаются другими исследованиями. В частности, в работе [66] приводятся результаты исследований реакции протокола OSPF на периодические многократные отказы каналов в области маршрутизации.

В работе [66] показано, что в условиях постоянных периодических отказов в сети, в конечном итоге статистическое распределение времени сходимости приходит к некоторому стационарному распределению (рис. 17).



а. б.

Рис. 17. Статистическое распределение времени сходимости сети OSPF в условиях периодических многократных отказов каналов [66]

Анализ графических зависимостей на рис. 17 показал, что, когда интервал Hello равен 10 с (значение по умолчанию), менее чем в 30% случаях время сходимости сети меньше 6 с, что соответствует единственной итерации пересчета путей за счет выполнения алгоритма SPF. В случаях, когда время сходимости находится в интервале 6-7 с, некоторое число маршрутизаторов выполняет 2 итерации вычисления алгоритма SPF (при *SPF_Delay_Timer*=1 с и *SPF_Hold_Timer*=1 с) из-за непрерывно приходящих LSA сообщений об изменениях топологии. Когда время сходимости составляет 8–9 с, это

соответствует ситуации, когда алгоритм SPF вычисляется трижды, при этом значение *SPF_Hold_Timer* (в соответствии с алгоритмом его экспоненциального роста) увеличивается до 2 с. Для случаев, когда время сходимости превышает 11 с, есть два объяснения. Первое – это происходит из-за тройного вычисления алгоритма SPF, в условиях, когда *SPF_Hold_Timer* увеличивается до 3 с. Второй вариант – вычисление алгоритма SPF происходит дважды, при этом второе вычисление задерживается в соответствии с *SPF_Hold_Timer*=5 с, что приводит к итоговому времени сходимости 11 с. В общем результаты, представленные в работе [66], показывают, что при интервале Hello равном 10 с, для обеспечения сходимости сети в 50% случаев необходимо более 10 с.

Анализируя причины динамики роста времени сходимости в условиях периодических отказов, авторы работы [66] приходят к выводу, что основной причиной такой динамики является многократность отказов и их асинхронность относительно временных параметров протокола. Авторы отмечают, что сценарии периодических «каскадов» отказов каналов могут служить причиной блокировки сети в результате перехода ее в режим перманентного пересчета изменений топологии.

Особый интерес представляют исследования с одинаковыми исходными данными, проведенные как в среде моделировании OPNET, так и на реальном телекоммуникационном оборудовании. Их анализ позволяет оценить адекватность моделирования в OPNET и погрешность результатов моделирования в этой среде.

В работе [67] представлены исследования времени сходимости сети на основе моделирования как в среде OPNET, так и экспериментальных исследований для протоколов RIP, OSPF и EIGRP. Также в данном исследовании представлены выводы о влиянии отказов сети на эффективность маршрутизации трафика, критичного к задержкам (видео и речи). Временные параметры протоколов были настроены по умолчанию. Топология исследуемой сети представлена на рис. 18.

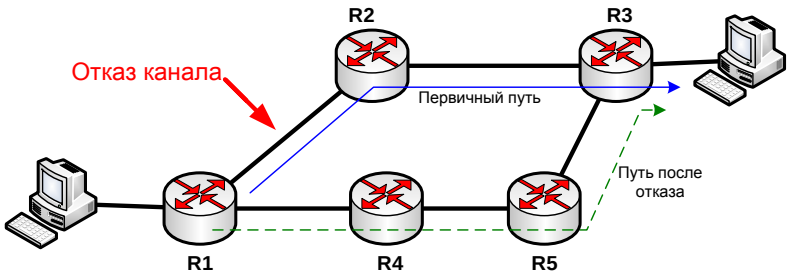


Рис. 18. Топология исследуемой сети в работе [67]

Результаты исследования времени сходимости протоколов для топологии на рис. 18 при моделировании в среде OPNET и при экспериментальных исследованиях с использованием реального оборудования (маршрутизаторы – Cisco 2811, каналы связи – Ethernet 100Base-T) представлены в таблице 5.

Таблица 5 - Результаты исследования времени сходимости протоколов в среде OPNET [67]

Протокол маршрутизации	Время сходимости при первичной инициализации соединений в сети		Время сходимости при реконфигурации после отказа		
	Моделирование в OPNET	Эксперимент	Моделирование в OPNET	Эксперимент	Погрешность моделирования
RIP	11,01 с	-	8,66 с	13,66 с	62%
OSPF	10,75 с	-	5,01 с	6	20%
EIGRP	5,018 с	-	0,025 с	2,12	4300%

В работе [67] делается вывод о том, что различие в результатах, полученных на основе моделирования и в реальном эксперименте, достигает нескольких секунд. Так, моделирование протокола EIGRP в среде OPNET показывает, что протокол сходится в течение миллисекунд, но в эксперименте на реальном оборудовании на это требуется порядка 2 с. Такое расхождение, на взгляд авторов, обусловлено тем, что средство моделирования не учитывает время, которое требуется для идентификации отказа канала связи.

Дополнительно в работе [67] было исследовано влияние отказов сети на эффективность маршрутизации трафика, критичного к задержкам (видео и речи). Результаты данного моделирования представлены на рис. 18.

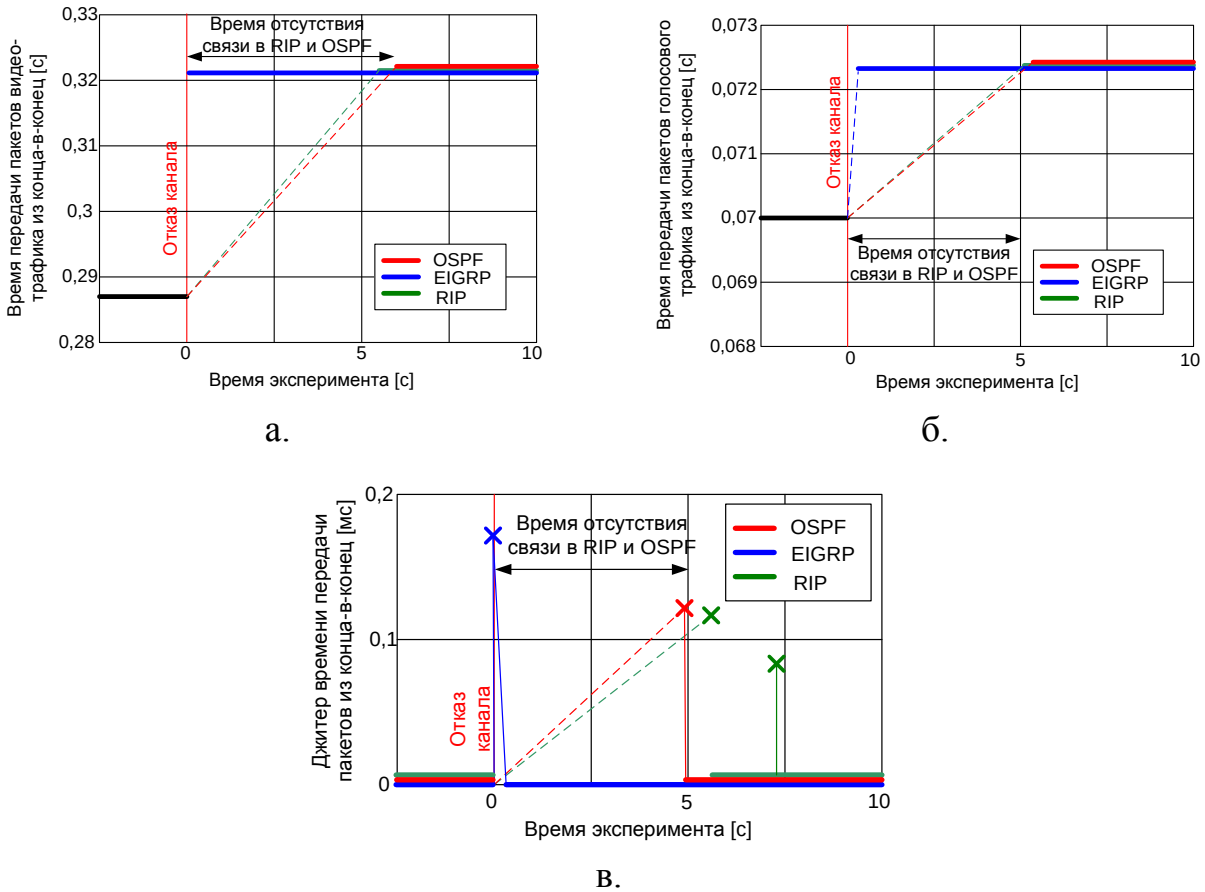


Рис. 18. Результаты исследования влияния отказов сети на эффективность маршрутизации трафика, критичного к задержкам (видео и речи) [67]

Проведенное моделирование в среде OPNET показало, что при использовании протоколов RIP и OSPF реконфигурация путей передачи потоков трафика в сети ведет к перерывам связи порядка 5 с. При этом после восстановления связи, передаваемым потокам характерно высокое значение джитера – 0,1…0,12 мс. Протокол EIGRP более устойчив к изменению топологии, и время перерыва связи для него составляет не более 0,05…0,1 с (рис. 18в) [67].

В работе [37] представлены результаты сравнительного анализа сходимости сети, использующей протоколы IS-IS и OSPF, на основе результатов моделирования в среде OPNET и экспериментов на маршрутизаторах Cisco 2500. В этой же работе был проведен анализ времени сходимости при условии использования обнаружителя отказа канала средствами протокола канального уровня (вариант протокола BFD). Исследовались варианты протоколов с таймерами по умолчанию. Моделируемая топология представлена на рис. 19. В таблице 6 представлены результаты моделирования сходимости сети для каналов с различной пропускной способности применительно к протоколам OSPF и IS-IS.

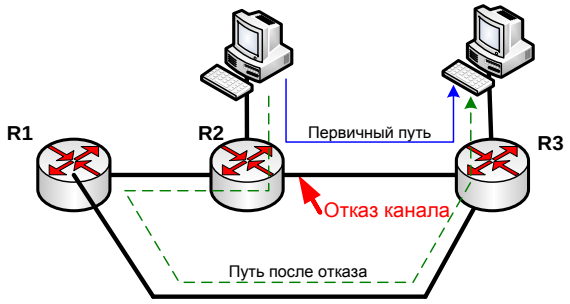


Рис. 19. Топология сети, исследуемая в работе [37]

Таблица 6 – Время сходимости сети для каналов с различной пропускной способности при использовании протоколов OSPF и IS-IS [37]

Пропускная способность каналов сети	Моделирование в OPNET [с]		Экспериментальные исследования [с]			
			без использования BDF		с использованием BDF	
	OSPF	IS-IS	OSPF	IS-IS	OSPF	IS-IS
64 кбит/с	13,279	1,0055	13,156	1,428	0,547	0,086
128 кбит/с	13,652	1,0027	12, 129	1,264	0,538	0,076
256 кбит/с	13,921	1,0025	13,101	1,126	0,537	0,065
512 кбит/с	13,344	1,0013	13,057	1,254	0,541	0,056
2,048 Мбит/с	12,995	1,0003	13,055	1,066	0,536	0,048

Основной вывод, который можно сделать по итогам анализа таблицы 6 – это инвариантность времени сходимости сети к пропускной способности каналов связи при их низкой загрузке, а также существенное снижение времени сходимости сети (на 93-95%) при использовании обнаружителя отказов канального уровня на основе протокола BDF.

Анализ погрешности моделирования в среде OPNET показал, что относительная погрешность при сравнении с экспериментальными данными составляет 2-11% для протокола OSPF и 22-40% для протокола IS-IS. Общим

выводом по результатам оценки погрешности может быть то, что относительная погрешность моделирования убывает с ростом значений пропускной способности каналов сети и увеличением значений временных параметров протокола. Это происходит из-за того, что длительность времени от момента отказа до момента его обнаружения, которая не учитывается средствами моделирования в OPNET, при увеличении указанных значений начинает играть все меньшую роль.

Кроме того, в работе [37] содержатся результаты исследования в среде OPNET модели смешанной сети из 93 маршрутизаторов с каналами различной пропускной способностью - от 9,6 кбит/с до 10 Мбит/с. При этом каналы 9,6 кбит/с, 14,4 кбит/с и 64 кбит/с составляли 90% топологии сети, а остальные 10% - каналы 2 Мбит/с и 10 Мбит/с. Максимальное время сходимости такой сети в случае отказа канала при использовании протокола OSPF составляет приблизительно 12 с, а для протокола IS-IS - приблизительно 70 с. В данной работе показано, что в моменты отказов в медленных каналах возникают перегрузки LSA сообщениями, приводящие к их потере, что, в свою очередь, приводит к лавинообразному нарастанию загрузки из-за новых попыток их передачи. Так в протоколе OSPF использование каналов 9,6 кбит/с и 14,4 кбит/с достигает 80-100%, каналов 64 кбит/с - 10-20%, а каналов 2 и 10 Мбит/с - менее 10%. При этом протокол IS-IS сходится за большее время из-за большей загрузки медленных каналов собственными сообщениями.

В работе [68] было проведено исследование эффективности протоколов OSFF и EIGRP в среде OPNET в условиях различной нагрузки на сеть, состоящей из 6 маршрутизаторов, соединенных общим каналом PPP_DS1 1,544 Мбит/с, а также исследование времени сходимости этих протоколов. К сожалению, автор работы не приводит полные данные об условиях эксперимента, однако в связи с тем, что данные в этой работе совпадают с ранее приведенными исследованиями, они приводятся в таблицах 7 и 8.

Таблица 7 – Оценка параметров эффективности сети, использующей протоколы EIGRP и OSPF [68]

Загрузка сети	Средняя задержка пакетов в сети [с]		Средняя задержка пакетов видеотрафика в сети в условиях QoS [с]		Потери пакетов	
	OSPF	EIGRP	OSPF	EIGRP	OSPF	EIGRP
0	$\approx 10^{-6}$		$\approx 2 \cdot 10^{-2}$		0 %	
20 %	$\approx 7 \cdot 10^{-4}$	$\approx 2 \cdot 10^{-5}$	$\approx 4 \cdot 10^{-2}$	$\approx 3 \cdot 10^{-2}$	0,35%	0,14%
40 %	≈20	≈2	≈3	≈1,5	6%	2,9%
60 %	≈27	≈10	≈3	≈5	нет данных	
80 %	≈30	≈20	≈7	≈7		

Таблица 8 – Оценка времени сходимости в сети, использующей протоколы EIGRP и OSPF при однократном изменении топологии [68]

Загрузка сети	Время сходимости сети	
	OSPF	EIGRP
40 %	≈5 с	≈0,3 с
80 %	≈15 с	≈7,5 с

В работе [69] рассматривалось экспериментальное исследование сходимости сети на основе технологии Frame Relay, имитирующие работу двух автономных областей маршрутизации с использованием протоколов OSPF и RIP. Для оценки времени сходимости авторами была построена экспериментальная сеть, представленная на рис. 20. Настройки протоколов в сети - по умолчанию. Диагностика времени сходимости сети ведется по маршруту R4-R7 (см. рис. 20).

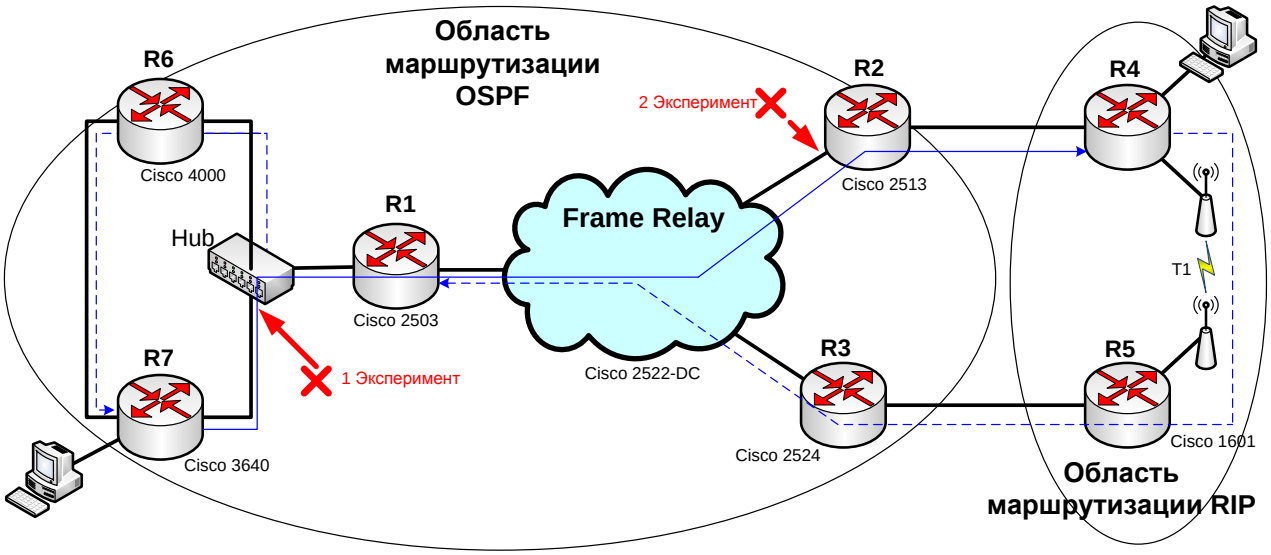


Рис. 20. Экспериментальная сеть, исследуемая в работе [69]

В первом эксперименте исключается связь R1-R7 за счет отключения соответствующего порта Ethernet коммутатора. В этом случае соединение R4-R7 реконфигурируется через R6. Время сходимости сети с протоколом OSPF при этом составляет 14±2 с, потери трафика на контролируемом маршруте - 7%.

Во втором эксперименте исключается связь R2-R1, за счет отключения соответствующего порта на маршрутизаторе R1. В этом случае соединение R4-R7 реконфигурируется через маршрутизаторы R3 и R5. В этом эксперименте авторами исследовались вопросы сходимости как сети в целом, так и отдельно сетей на основе протоколов OSPF и RIP, причем данные протоколы имеют различные временные параметры.

Результаты проведенных в работе [69] исследований сведены в таблицу 9.

Анализ результатов, проведенных в работе [69] экспериментов показывает слабое влияние изменения значений секундных таймеров на параметры сходимости внутри отдельных сетей. Возможно, это объясняется тем, что авторы не стали исследовать существенно более низкие значения таймеров в миллисекундном диапазоне, так как именно этот диапазон таймеров, как показывают исследования [1, 30, 73], позволяет обеспечить высокое время сходимости сети. При этом важным выводом является то, что время сходимости объединенной сети, построенной на протоколах с различными временными параметрами, составляет значения в 1,5-7 раз дольше, чем сходимость самых медленных сетей в ее составе, а потери трафика составляют от 20 до 40%. Данный вывод подтверждается похожими

результатами исследований [83, 84], которые показывают, что время сходимости объединенных сетей из нескольких автономных областей маршрутизации составляет не менее 50-200 с.

Таблица 9 – Результаты экспериментальных исследований объединенной сети на основе протоколов OSPF и RIP [69]

	Исследуемый объект	Параметры протокола				Время сходимости	Потери трафика
		Update Timer (Hello Interval)	Invalid Timer (Dead Interval)	Hold_Down Timer (Max Hold Timer)	Flush Timer (Таймер сброса в нач. значения)		
Тай-меры по умолча-нию	Сеть OSPF	10 с	40 с	5 с	5 с (?)	14±2 с	7%
	Сеть RIP	30 с	180 с	180 с	240 с	105±5 с	53%
	Сеть в целом					472 с	23%
Быстрые таймеры	Сеть OSPF	5 с	10 с	10 с	30 с	11,8 с	5,9%
	Сеть RIP	5 с	10 с	10 с	30 с	119,8 с	59,9%
	Сеть в целом					138 с	69,1%
Медлен-ные таймеры	Сеть OSPF	60 с	360 с	360 с	480 с	11,6 с	5,8 %
	Сеть RIP	60 с	360 с	360 с	480 с	120 с	63%
	Сеть в целом					867,8 с	43,3%

В работе [70] были проведены экспериментальные исследования времени сходимости протокола OSPF-TE в оптической транспортной сети GMPLS в случае, когда пути коммутации меток LSP (Label Switch Path) в сети уже установлены, и они вынужденно перенаправляются в результате отказа единственного канала связи. Топология экспериментальной сети представлена на рис. 21.

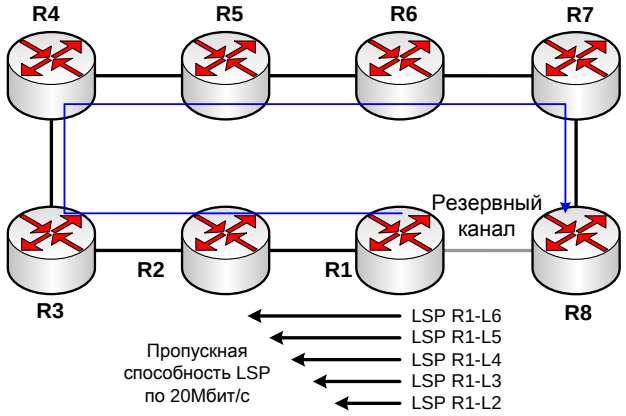
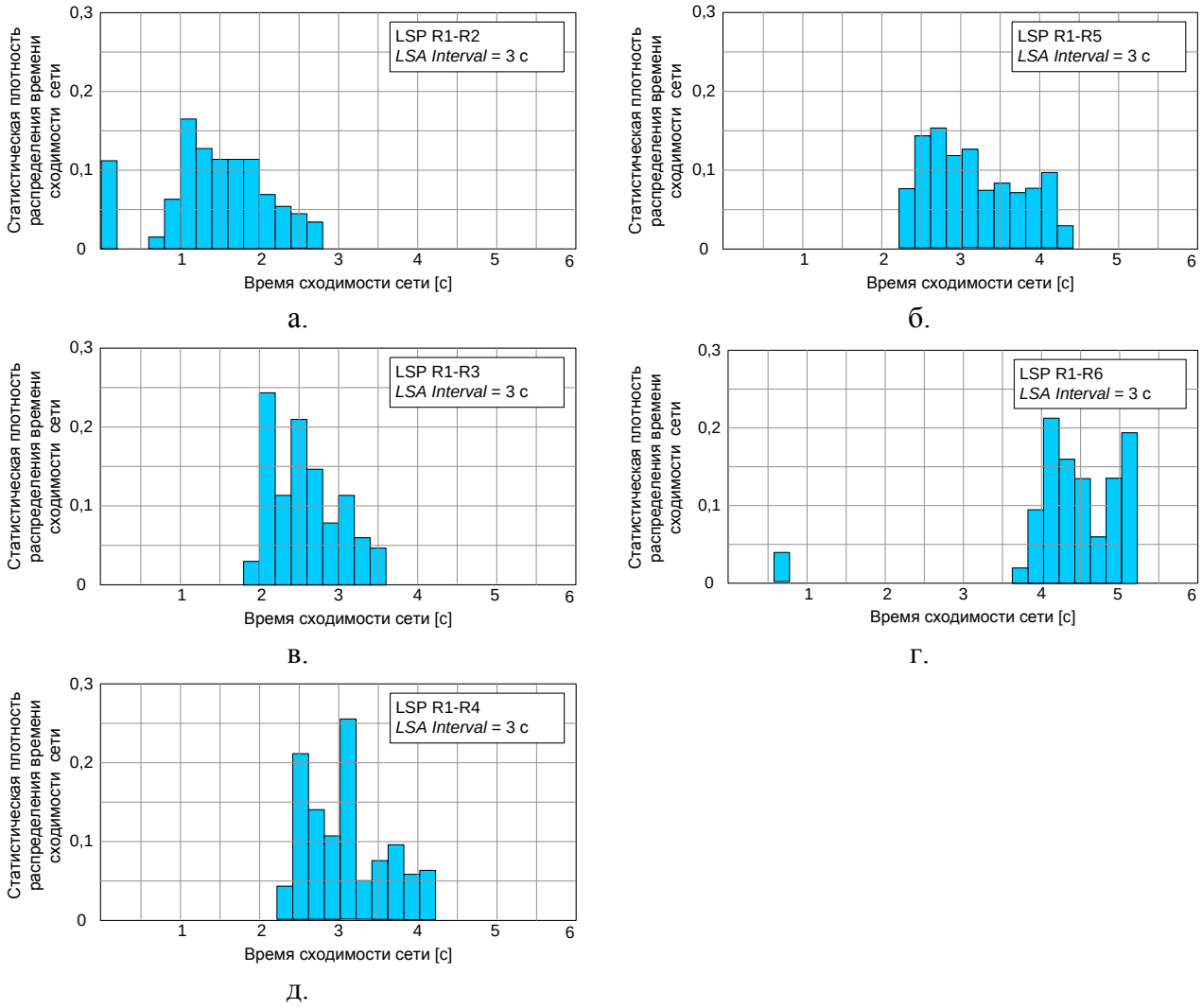


Рис. 21. Модель оптической транспортной сети на основе протокола OSPF-TE, исследуемая в работе [70]

Распределение статистических оценок времени сходимости при первоначальном установлении путей LSP при многократном моделировании сети GMPLS (на рис. 21) представлено на рис. 22.

Периодичность генерации LSA сообщений о доступности узлов в протоколе OSPF-TE достигает значения до 3 с и является основным фактором, определяющим время сходимости сети. Увеличение периода рассылки

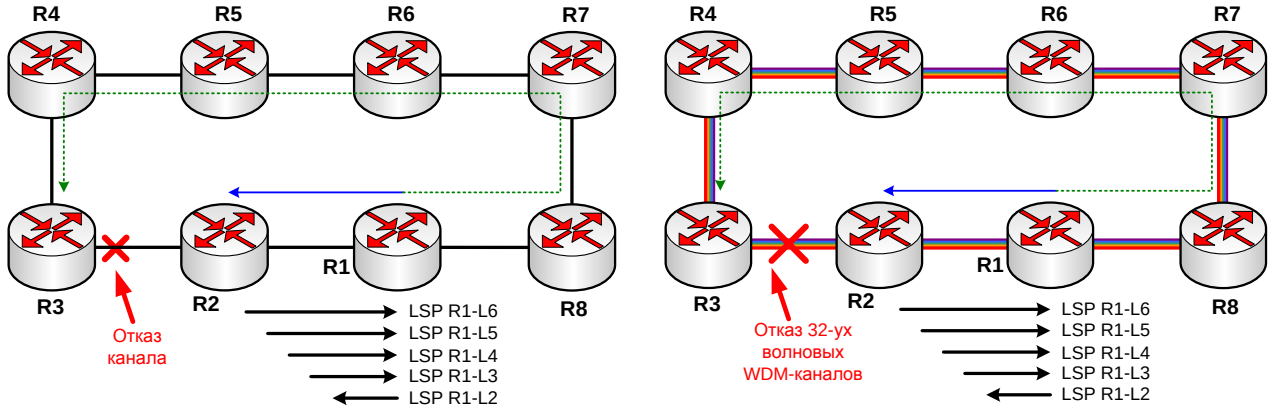
сообщений LSA приводит к более длительному времени сходимости. Как показано на рис. 22(е), время сходимости приблизительно 5 с необходимо для LSP с 5 транзитными участками (от R1 до R6).



а. б. в. г. д.

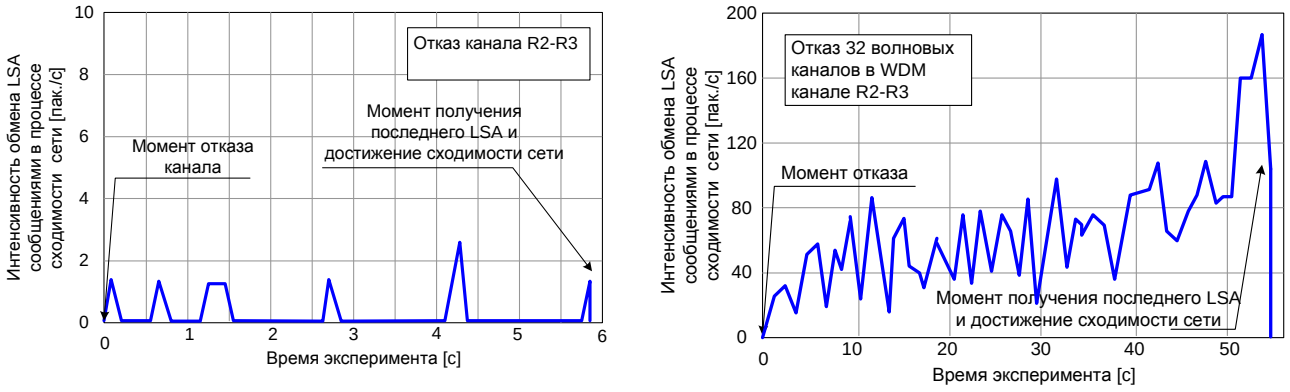
Рис. 22. Распределение статистических оценок времени сходимости при первоначальном установлении путей LSP в сети OSPF-TE [70]

В работе [70] было проведено исследование времени сходимости при моделировании как случаев отказа канала связи (рис. 23а), так и случаев отказа «цветных» подканалов отдельных длин волн в общем WDM-канале (рис. 23б). Интенсивность распространения сообщений LSA, порождаемых отказами для обоих этих случаев приведены на рис. 24а и 24б, соответственно. Общие характеристики процессов сходимости сети при двух видах рассматриваемых отказов приведены в таблице 10.



а. б.

Рис. 23. Моделирование случаев отказа канала связи (а) и отказа подканалов отдельных длин волн в WDM-канале (б) [70]



а. б.

Рис. 24. Интенсивность распространения LSA сообщений, порождаемых отказами в канале связи, для случаев отказа канала связи (а) и отказа подканалов отдельных длин волн в WDM-канале (б) [70]

Таблица 10 – Характеристики процессов сходимости сети OSPF-TE [70]

	Случай отказа канала связи	Случай отказа подканалов отдельных длин волн в WDM-канале
Кол-во пакетов OSPF-TE	10	около 3400
Новые LSA сообщения	14	448
Сообщения LSA об обновлении путей	5	около 27000
Время сходимости сети	≈6 с	≈55 с

По итогам проведенного исследования в работе [70] сделаны выводы о том, что:

- время сходимости транспортной сети OSPF-TE сопоставимо с временем сходимости стандартной сети OSPF при схожей топологической сложности и одинаковой пропускной способности каналов связи;

- в случае отказа отдельный «цветных» каналов в WDM сети, время сходимости на порядок больше, чем для стандартной транспортной сети OSPF-TE без WDM. При этом доминирующим фактором, определяющем высокую длительность сходимости, является задержка синхронизации баз данных OSPF-TE, содержащих информацию о пропускных способностях отдельных WDM каналов.

Особенностью протокола OSPF-TE является необходимость поддержания в актуальном и синхронном состоянии баз данных TE о путях LSP для передачи трафика. Фактически, время сходимости в транспортной сети OSPF-TE характеризуется восстановлением синхронизации этих баз на всех маршрутизаторах сети. Данное время может зависеть как от топологических характеристик сети, так и от принятой в сети политики инжиниринга трафика. Политика инжиниринга трафика существенно влияет на сходимость, так как зачастую в транспортной сети функционируют множество наложенных виртуальных сетей, задачи маршрутизации в которых решаются с учетом приоритетности трафика, его требований к качеству обслуживания, динамически установленных виртуальных каналов и т.д. При этом, после отказа требуется восстановление работоспособности не только физической сети, но и всех наложенных виртуальных сетей.

Таким образом, общими выводами по результатам анализа исследований [30, 37, 65-70] в области сходимости сетей может быть следующее:

- задержка сходимости определяется временными параметрами протокола маршрутизации, топологией сети и пропускной способностью каналов связи;
- время сходимости сети в зависимости от топологической сложности сети для протоколов маршрутизации составляет от нескольких до десятков секунд;
- при наличии периодических групповых отказов каналов связи, время сходимости сети существенно увеличивается и стремится к стационарному статистическом распределению.

Перспективные направления исследований, ориентированных на снижение времени сходимости сети

Проведенный анализ принципов функционирования и реакции протоколов маршрутизации на отказы в сети, а также исследований в области оценки сходимости сети показал несовершенство существующих технологических решений в этой области. Как показал анализ, представленный в работах [30, 66], к наиболее сложным условиям функционирования протоколов маршрутизации относится наличие периодических групповых отказов элементов сети. Причиной таких групповых отказов могут быть изменения отношения сигнал-шум в отдельных радиоканалах, входящих в состав сети, что показано в работах [37, 71]. В таких условиях различными исследователями предложены новые направления решения задачи снижения времени сходимости и повышения устойчивости сети. К ученым, ведущим исследования в области анализа времени сходимости сетей, относятся:

Goyal M. [1, 31, 36, 72], Hosseini S. H. [1, 31, 36], Trivedi K. [1, 36], Shaikh A. [1, 36, 50], Choudhury G. [1, 36, 74], Xie W. [31, 36], Xin L. [39, 75], Ramakrishnan K. K. [72] и др. Ниже представлен обзор основных публикаций о перспективных направлениях и способах снижения времени сходимости сетей.

В работах [33, 39] предложены динамические механизмы изменения таймера Hello в протоколе OSPF, основанные на экспериментальных исследованиях авторов. Предложенный в работе [39] способ повышения сходимости основан на уменьшении интервала Hello по экспоненте каждый раз, когда количество потерянных Hello сообщений превышает заданный порог. Подобный способ описан и в работе [33], где предложена динамическая коррекция интервала ожидания восстановления связи (Dead Time), основанная на оценке уровня потерь Hello-сообщений за определенный период времени.

В работе [72] показано, что сходимость сети определяется средней сетевой связностью топологии, загрузкой сети и таймером для интервала Hello. Этот вывод также подтверждается результатами исследований, представленных в работах [1, 30, 73].

В работе [1] представлены результаты оптимального подбора значения для таймера Hello для протокола OSPF. В этой работе утверждается, что для устойчивости сети рациональным значением таймера Hello является 500 мс, что соответствует времени сходимости сети примерно в 2 с. Авторами отмечается, что дальнейшее снижение периода Hello ведет к потере устойчивости сети. В работе предлагается дополнительно ускорить сходимость, за счет приоритетной обработки пакетов Hello по отношению к другим типам сообщений OSPF, а также за счет динамически меняющихся значений времени генерации сообщений LSA и задержек вычисления алгоритма поиска путей SPF.

В работе [73] представлены результаты экспериментальных исследований по подбору оптимального значения интервала диагностики состояния смежных каналов путем рассылки пакетов Hello. Результаты моделирования в сети, состоящей из 292 узлов и 765 каналов связи, показывают шестикратное увеличение числа флуктуаций маршрутов при уменьшении Hello таймера от 500 мс до 250 мс. При этом авторы допускают, что в интересах обеспечения быстрой сходимости, интервал Hello может быть уменьшен до 275 мс, при обеспечении устойчивости сети в приемлемых пределах.

В работе [30] исследованы возможности применения в протоколе OSPF миллисекундных таймеров (1 мс для интервала рассылки сообщений Hello, и 4 мс для интервала ожидания восстановления связи (Dead Time), а также влияние таких сверхкоротких интервалов на устойчивость сетей OSPF.

В работе [74] указывается, что снижение интервала рассылки сообщений Hello с одной стороны приводит к увеличению точности диагностики отказов в сети, но с другой стороны - возрастает количество ложных тревог, которые ведут к дополнительным циклам пересчета путей, что снижает коэффициент готовности сети. При этом, как показано в работе [72], интенсивность ложных тревог увеличивается пропорционально уровню нагрузки сети и числу каналов в ней. Таким образом, оптимальное значение интервала Hello зависит от

допустимого уровня вероятности ложной тревоги, ожидаемых уровней нагрузки сети и ее топологической сложности.

Несколько другое направление повышения скорости сходимости представлено в работах [14-17, 36, 75-83], направленных не на поиск оптимальных временных параметров алгоритмов маршрутизации, а на совершенствование механизмов самого алгоритма SPF.

В работе [75] предлагается способ снижения времени сходимости сети за счет уменьшения размеров обновления таблицы маршрутизации. Данный способ, названый авторами «инкрементным обновлением FIB» (iFIB), вместо того, чтобы выводить в оперативную память таблицу маршрутизации целиком всякий раз, когда происходят изменения топологии, предусматривает выборочное обновление в таблице FIB только тех маршрутов или префиксов сетей, на которые влияет произошедшие топологическое изменение. Данный способ является развитием подхода, использованного в алгоритме iSPF, а сам способ предлагается к использованию совместно с алгоритмом iSPF, что позволит значительно уменьшить время сходимости сети.

В работах [14-17, 76] для сокращения времени перехода на новый маршрут предложены различные варианты расчета резервных путей, а также их выбора при отказе текущего маршрута, входящего в состав дерева кратчайших путей SPT. Это позволяет маршрутизатору, который идентифицировал отказ, сначала осуществить реконфигурацию маршрутов, а уже потом приступить к рассылке LSA сообщений и запуску алгоритма SPF для расчета кратчайших путей. В частности, в работах [14-17] предложены варианты сокращения вычислительной сложности выполнения алгоритма SPF за счет парных перестановок маршрутов, при выборе резервных путей.

Имеются работы по обобщению самого алгоритма Дейкстры (как правило, используемого в качестве основы алгоритма SPF) в направлении использования его для формирования как кратчайших, так и резервных путей [76], а также по динамическому исправлению ранее рассчитанного дерева кратчайших путей SPT после изменения топологии сети [78-81].

В работе [82] предлагается периодически кэшировать результаты работы алгоритма SPF и использовать кэшируемую информацию в случае восстановления отказавшего канала или узла без повторного пересчета топологии. Кроме того, кэширование позволяет передавать минимальное количество данных между маршрутизаторами, которые используются для синхронизации баз данных о кэшированных состояниях топологии.

Чрезвычайно интересным способом является так называемая «корреляция LSA», которая является способом оптимизации вычисления SPF, предложенным в работе [36] и развивающим способ проверки каждого получаемого LSA на логическую связь с ранее полученными LSA-сообщениями, определенного в RFC 2328 [32]. В работе [36] авторами показано, что параметры задержки вычисления алгоритма SPF, которые используют фиксированный или экспоненциально замедляющийся временной интервал, неэффективны в случаях, если изменения происходят в одних и тех же каналах. В данной работе предлагается использовать отдельные LSA

сообщения, но не в качестве признака изменения топологии (с последующей инициализацией пересчета SPF), а в качестве признака нестабильного состояния канала или области сети. Предлагается механизм, при котором отдельные LSA сообщения не будут приводить к расчету алгоритма SPF, а будут накапливаться в течение определенного интервала и анализироваться на предмет поиска корреляционных зависимостей в изменении топологии. Вычисление такой корреляционной зависимости позволит определить область смежных узлов, рассылающих LSA из-за нестабильного состояния каналов между ними, а также возможные общие дестабилизирующие факторы, воздействующие на отдельные области сети. Данный подход позволяет провести анализ изменений топологии сети в целом на некотором промежутке времени и установить общие закономерности этого процесса. Авторами предложен корреляционный анализ по следующим параметрам: идентификаторы каналов; идентификаторы узлов; параметры данных, передаваемых по каналам связи и др. В случае выявления корреляционных закономерностей в процессе изменения топологии сети, инициируется алгоритм SPF с целью формирования дерева путей, исключающих область топологических изменений.

Фактически, подход, предложенный авторами работы [36], может быть положен в основу целого комплекса способов обнаружения преднамеренных деструктивных воздействий, направленных на дестабилизацию сети связи за счет преднамеренного деструктивного воздействия на ее отдельные каналы и узлы.

Заключение

Результаты обобщенного анализа принципов функционирования протоколов маршрутизации, а также влияния их временных параметров на время сходимости сети, представленные в статье, могут быть использованы для обоснования новых алгоритмических решений при маршрутизации трафика в сетях, на которые воздействуют различного рода дестабилизирующие факторы. Представленный в работе анализ перспективных направлений совершенствования протоколов маршрутизации может быть использован для совершенствования таких протоколов как: OSPF, OSPF-TE, IS-IS, IGRP, EIGRP. Кроме того, ряд рассматриваемых в статье решений может быть положен в основу разработки протоколов маршрутизации для мобильных MANET сетей, построенных на основе Mesh-технологий.

Исследования эффективности функционирования протоколов маршрутизации сетей связи выполнены при государственной поддержке РФФИ инициативного научного проекта № 13-07-97518 и поддержке Департаментом приоритетных направлений науки и технологий Минобрнауки РФ – грантом Президента РФ № МК-755.2012.10.

Автор выражает благодарность Михайлову Р.Л. за плодотворное обсуждение материалов и помощь в подготовке текста статьи.

Литература

1. Goyal M., Soperi M., Baccelli E., Choudhury G., Shaikh A., Hosseini S. H., Trivedi K. Improving Convergence Speed and Scalability in OSPF: A Survey // IEEE Communications Surveys & Tutorials. 2012. № 14 (2). pp. 443-463. doi: 10.1109/SURV.2011.011411.00065. HAL Id: hal-00651596. URL: https://hal.archives-ouvertes.fr/hal- 00651596 (дата доступа 01.05.2015).

2. Markopoulo A., Iannaccone G., Bhattacharya S., Chua C., Ganjali Y., Diot C. Characterization of failures in an operational IP backbone network // IEEE/ACM Transactions on Networking. 2008. vol. 16. № 4.

3. Labovitz C., Ahuja A., Jahanian F. Experimental study of internet stability and backbone failures // Proc. The 29-th International Symposium on Fault-Tolerant Computing. – Madison (WI, USA), 1999. – pp. 278-285. doi: 10.1109/FTCS.1999.781062

4. Ganjali Y., Bhattacharyya S., Diot C. Limiting the impact of failures on network performance // Sprint ATL Tech. Res. Rep., Tech. Rep. RR04-ATL-020666, 2003. - URL: https://research.sprintlabs.com/publications/uploads/RR04-ATL-020666.pdf (дата доступа 01.05.2015).

5. Поповский В. В., Волотка В. С. Методы анализа динамических структур телекоммуникационных систем // Восточно-Европейский журнал передовых технологий. 2013. № 5/2 (65). С. 18-22.

6. Поповский В. В., Волотка В. С. Математическое моделирование надежности инфокоммуникационных систем // Телекомунікаційні та інформаційні технології. 2014. № 3. С. 5-9.

7. Поповский В. В., Лемешко А. В., Мельникова Л. И., Андрушко Д. В. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника. 2005. Т. 4. № 4. С. 372-382. – URL: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (дата доступа 01.05.2015).

8. Лемешко А. В., Евсеева О. Ю., Дробот О. А. Методика выбора независимых путей с определением их количества при решении задач многопутевой маршрутизации // Праці УНДІРТ. 2006. № 4 (48). С. 69-73. – URL: http://alem.ucoz.ua/_ld/0/14_Lemeshko_UNIIRT.pdf (дата доступа 01.05.2015).

9. Лемешко А. В., Козлова Е. В., Романюк А. А. Математическая модель отказоустойчивой маршрутизации, представленная алгебраическим уравнениями состояния MPLS-сети // Системи обробки інформації. 2013. № 2 (109). С. 217-220.

10. Попков В. К. Математические модели связности. Новосибирск: Изд. ИВМиМГ СО РАН, 2006. 490 с.

11. Попков В. К., Блукке В. П., Дворкин А. Б. Модели анализа устойчивости и живучести информационных сетей // Проблемы информатики. 2009. № 4. С. 63-78.

12. Сорокин А. А., Дмитриев В. Н. Описание систем связи с динамической топологией сети при помощи модели «мерцающего» графа //

Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2009. № 2. С. 134-139.

13. Сорокин А. А., Дмитриев В. Н., Чан Куок Тоан, Резников П. С. Оценка результатов использования протокола RIP в системах связи с динамической топологией сети методом имитационного моделирования // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2014. № 4. С. 85-93.

14. Перепелкин Д. А. Алгоритм парных перестановок маршрутов на базе протокола OSPF при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2014. № 1 (47). С. 84-91.

15. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации? на базе протокола IGRP при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2012. № 4 (42). С. 33-38.

16. Перепелкин Д. А. Динамическое формирование структуры и параметров линий связи корпоративной сети на основе данных о парных перестановках маршрутов // Информационные технологии. 2014. № 4. С. 52-60.

17. Корячко В. П., Перепелкин Д. А. Анализ и проектирование маршрутов передачи данных в корпоративных сетях. М.: Горячая линия – Телеком, 2012. 236 с.

18. Мейкшан В. И. Анализ влияния отказов оборудования на функционирование мультисервисной сети с адаптивной маршрутизацией // Доклады академии наук высшей школы Российской Федерации. Технические науки. 2010. № 2 (15). С. 69-80.

19. Горев П. Г., Назаров А. С., Пасечников И. И. Определение связности в путевом пространстве состояний телекоммуникационной сети // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2012. Т. 17. № 5. С. 1360-1363.

20. Литвинов К. А., Пасечников И. И. Подходы к решению задачи маршрутизации в современных телекоммуникационных системах // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. № 1. С. 64-69.

21. Синтез и анализ живучести сетевых систем: монография / Ю. Ю. Громов, В. О. Драчев, К. А. Набатов, О. Г. Иванова. М.: «Издательство Машиностроение-1», 2007. 152 с.

22 Ковальков Д. А. Математические модели оценки надежности мультисервисного узла доступа // Радиотехнические и телекоммуникационные системы. 2011. № 2. С. 64-71.

23. Горбунов И. Э. Методология анализа и синтеза реконфигурируемых топологий мобильной связи // Математичні машини і системи. 2006. № 2. С. 48-59.

24. Егунов М. М., Шувалов В. П. Анализ структурной надёжности транспортной сети // Вестник СибГУТИ. 2012. № 1. С. 54-60.

25. Макаренко С. И. Анализ воздействия преднамеренных помех на сетевой уровень модели взаимодействия открытых систем и функционирование протокола маршрутизации оценки состояния канала (OSPF) // Информационные технологии моделирования и управления. 2009. № 7 (59). С. 956-961.

26. Макаренко С. И. Анализ воздействия преднамеренных помех на функционирование расширенного протокола маршрутизации внутреннего шлюза (EIGRP) // Информационные технологии моделирования и управления. 2010. № 2 (61). С. 223-229.

27. Бачинский В. А., Гиоргизова-Гай В. Ш. Выбор протокола динамической маршрутизации в корпоративной ip-сети // Системні дослідження та інформаційні технології. 2011. № 1. С. 99-110.

28. Султанахметов Д. Быстрая сходимость OSPF. Таймеры протокола OSPF // Network-Lab [Электронный ресурс]. 09.01.2014. URL: http://network-lab.ru/byistraya-shodimost-ospf-taymeryi-protokola-ospf/ (дата доступа 01.05.2015).

29. Moy J. T. OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley Professional, 1998. 338 p.

30. Tsegaye Y., Geberehana T. OSPF Convergence Times. Master of Science Thesis in the Programme Networks and Distributed Systems. Chalmers University of Technology. Göteborg (Sweden), 2012. 77 p. URL: http://publications.lib.chalmers.se/records/fulltext/184363/184363.pdf (дата доступа 01.05.2015).

31. Goyal M., Xie W., Hosseini S. H., Vairavan K., Rohm D. Improving OSPF Dynamics on a Broadcast LAN // Simulation. 2006. vol. 82. № 2. pp. 107-129. doi: 10.1177/0037549706065924

32. Moy J. RFC 2328. OSPF Version 2 // Network Working Group. Request for Comments. Ascend Communications Inc, 1998.

33. Amir S., Biswajit N. Improving Network Convergence Time and Network Stability of an OSPF-Routed IP Network // Lecture Notes in Computer Science. 2005. Vol. 3462. pp. 469-485. doi: 10.1007/11422778_38

34. Choudhury G. RFC 4222. Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance // Network Working Group, Request for Comments. AT&T Publ., 2005.

35. Cisco IOS Release 12.2(14)S. OSPF Update Packet-Pacing Configurable Timers // Cisco [Электронный ресурс], 2010. URL: http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fsospfct.html (дата доступа 01.05.2015).

36. Goyal M., Xie W., Soperi M., Hosseini S. H., Vairavan K. Scheduling routing table calculations to achieve fast convergence in OSPF protocol // Proc. IEEE BROADNETS 2007. 2007. pp. 863–872. doi: 10.1109/BROADNETS.2007.4550524

37. Zaballos A., Seguí C. Analysis and simulation of IGP routing protocols // University Ramon Llull (La Salle Engineering), Barcelona (Spain). 2006. URL: http://users.salleurl.edu/~zaballos/opnet/Trame.pdf (дата доступа 01.05.2015).

38. Alaettinoglu C., Jacobson V., Yu H. Towards milli-second IGP convergence // IETF Draft. – 2000.

39. Fang W., Shanzhi C., Xin L., Yuhong L. A Route Flap Suppression Mechanism Based on Dynamic Timers in OSPF Network // The 9-th International Conference for Young Computer Scientists - IEEE, 2008.

40. Katz D., Ward D. RFC 5880. Bidirectional forwarding detection (BFD) // Internet Engineering Task Force, Request For Comments (Standards Track), 2010.

41. Bidirectional Forwarding Detection for OSPF. Cisco, 2005. 18 p. URL: https://www.cisco.com/en/US/technologies/tk648/tk365/tk480/technologies_white_paper0900aecd80244005.pdf (дата доступа 01.05.2015).

42. Cisco IOS Software Releases 12.0 S. IP Event dampening. // Cisco [Электронный ресурс], 2010. URL: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/s_ipevdp.html (дата доступа 01.05.2015).

43. Kolon M. C., Doyle J., Christensen S. The Complete Reference Juniper Network Routers. McGraw-Hill Osborne Media, 2002.

44. Baccelli E., Jacquet P., Nguyen D., Clausen T. RFC 5449. OSPF multipoint relay (MPR) extension for ad hoc networks // Internet Engineering Task Force, Request For Comments (Experimental). LIX, Ecole Polytechnique, 2009.

45. Roy A., Chandra M. RFC 5820. Extensions to OSPF to support mobile ad hoc networking // Internet Engineering Task Force, Request for Comments (Experimental), 2010.

46. Ogier R., Spagnolo P. RFC 5614. Mobile Ad-Hoc network MANET extension of OSPF using connected dominating set CDS flooding // Internet Engineering Task Force, Request for Comments (Experimental), 2009.

47. Raj A., Ibe O. A Survey of IP and Multiprotocol Label Switching Fast Reroute Schemes // Comput. Netw. 2007. vol. 51. № 8. pp. 1882–1907.

48. Rosen E., Viswanathan A., Callon R., RFC 3031. Multiprotocol label switching architecture // Internet Engineering Task Force, Request for Comments (Standards Track), 2001.

49. Davie B., Rekhter Y. MPLS: Technology and Applications. Morgan Kaufmann, 2000. 287 p.

50. Shaikh A., Wang D., Li G., Yates J., Kalmanek C. An efficient algorithm for OSPF subnet aggregation // Proc. 11-th IEEE International Conference on Network Protocols (ICNP), 2003. pp. 200-209. doi: 10.1109/ICNP.2003.1249771

51. Coltun R., Ferguson D., Moy J., Lindem A. RFC 5340. OSPF for IPv6 // Internet Engineering Task Force, Request for Comments (Standards Track), 2001. URL: http://www.rfc-editor.org/rfc/rfc5340.txt (дата доступа 01.05.2015).

52. Moy J., Pillay-Esnault P., Lindem A. RFC 3623. Graceful OSPF Restart // Network Working Group, Request for Comments, 2003. URL: https://tools.ietf.org/html/rfc3623 (дата доступа 01.05.2015).

53. Li T., Cole B., Morton P., Li D. RFC 2281. Cisco Hot Standby Router Protocol (HSRP) // Network Working Group, Request for Comments (Informational), 1998. URL: http://www.ietf.org/rfc/rfc2281.txt (дата доступа 01.05.2015).

54. Гребешков А. Ю. Управление сетями электросвязи по стандарту TMN: учеб. пособие. – М.: Радио и связь, 2004. – 156 с.

55. Kompella K., Rekhter Y. RFC 4203. OSPF extensions in support of generalized multi-protocol label switching (GMPLS) // Internet Engineering Task Force, Request for Comments (Standards Track), 2005. URL: https://www.ietf.org/rfc/rfc4203.txt (дата доступа 01.05.2015)

56. Pan P., Swallow G., Atlas A. RFC 4090. Fast reroute extensions to RSVP-TE for LSP tunnels // Internet Engineering Task Force, Request for Comments (Standards Track), 2005.

57. Atlas A., Zinin A. RFC 5286. Basic specification for IP fast reroute: Loop-free alternates // Internet Engineering Task Force, Request for Comments (Standards Track), 2008.

58. Shand M., Bryant S. RFC 5714. IP fast reroute framework // Internet Engineering Task Force, Request for Comments (Informational), 2010.

59. Shand M., Bryant S., Previdi S., IP fast reroute using not-via addresses // Network Working Group, Internet-Draft (Experimental), 2010. URL: https://tools.ietf.org/html/draft-ietf-rtgwg-ipfrr-notvia-addresses-06 (дата доступа 01.05.2015).

60. Atlas A. U-turn alternates for IP/LDP fast-reroute // Network Working Group, Internet-Draft (Experimental), 2006. URL: https://tools.ietf.org/html/draft-atlas-ip-local-protect-uturn-03 (дата доступа 01.05.2015).

61. Psenak P., Mirtorabi S., Roy A., Nguyen L., Pillay-Esnault P. RFC 4915. Multi-topology (MT) routing in OSPF // Internet Engineering Task Force, Request For Comments (Standards Track), 2007.

62. Simpson W. RFC 1853. IP in IP tunneling // Internet Engineering Task Force, Request For Comments (Informational), 1995.

63. Hanks S., Li T., Farinacci D., Traina P. RFC 1701. Generic routing encapsulation (GRE) // Internet Engineering Task Force, Request for Comments (Informational), 1994.

64. Ayari N., Barbaron D., Lefevre L., Primet P. Fault tolerance for highly available internet services: concepts, approaches, and issues // IEEE Communication Surveys and Tutorials. 2008. vol. 10. № 2. pp. 34-46. doi: 10.1109/COMST.2008.4564478

65. Dilber M. N., Raza A. Analysis of successive Link Failures effect on RIP and OSPF Convergence time delay // International Journal of Advances in Science and Technology. 2014. pp. 42-48. URL: http://sciencepublication.org /documents/sp/7.pdf (дата доступа 01.05.2015).

66. Zhao D., Hu X., Wu C. A Study on the Impact of Multiple Failures on OSPF Convergence // International Journal of Hybrid Information Technology. 2013. vol. 6. № 3. pp. 75-74. URL: http://www.sersc.org/journals/IJHIT/ vol6_no3_2013/7.pdf (дата доступа 01.05.2015).

67. Sankar D., Lancaster D. Routing Protocol Convergence Comparison using Simulation and Real Equipment // Advances in Communications, Computing, Networks and Security. 2013. Vol. 10. pp. 186-194.

68. Антонова А.А. Оценка эффективности протоколов динамической маршрутизации при передаче потокового видео // Автоматизация и управление

в технических системах. 2013. № 4.2. URL: http://auts.esrae.ru/7-151 (дата обращения: 02.05.2015). doi: 10.12731/2306-1561-2013-4-36

69. Pun H. Convergence Behavior of RIP and OSPF Network Protocols. Ph.D. thesis. B.A.Sc., University of British Columbia. 2001. 59 p. URL: http://www2.ensc.sfu.ca/~ljilja/cnl/pdf/hubert.pdf (дата обращения: 02.05.2015).

70. Huang S., Kitayama K., Cugini F., Paolucci F., Giorgetti A., Valcarenghi L., Castoldi P. An Experimental Analysis on OSPF-TE Convergence Time // Asia Pacific Optical Communications – International Society for Optics and Photonics. 2008. Vol. 7137. doi: 10.1117/12.803224

71. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально–помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. URL: http://jre.cplire.ru/jre/oct14/3/text.pdf (дата доступа 01.03.2015)

72. Goyal M., Ramakrishnan K. K., Feng W. Achieving Faster Failure Detection in OSPF Networks // Proc. IEEE International Conference on Communications (ICC-2003). 2003. Vol. 1. pp. 296-300. doi: 10.1109/ICC.2003.1204188

73. Basu A., Riecke J. Stability issues in OSPF routing // ACM SIGCOMM Computer Communication Review. 2001. Vol. 31. № 4. pp. 225-236.

74. Choudhury G., Ash G., Manral V., Maunder A., Sapozhnikova V., Prioritized treatment of specific OSPF packets and congestion avoidance: algorithms and simulations // Technical Report. AT&T, Tech. Rep. Publ., 2003.

75. Liu Y., Zhao X., Nam K., Wang L., Zhang B. Incremental For warding Table Aggregation // GLOBECOM 2010. Miami, Florida, USA, 2010. pp. 1-6.

76. Цветков К. Ю., Макаренко С. И., Михайлов Р. Л. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-телекоммуникационных сетей // Информационно-управляющие системы. 2014. № 2(69). С. 71-78.

77. Pu J., Manning E., Shoja G. C., Routing Reliability Analysis of Partially Disjoint Paths // Proc. IEEE Conference on Communications, Computers, and Signal Processing. Victoria, BC, Canada. 2001. Vol. 1. pp. 79-82.

78. McQuillan J., Richer I., Rosen E. The New Routing Algorithm for the ARPANET // IEEE Transactions on Communications. Vol. 28. № 5. 1980.

79. Franciosa P., Frigioni D., Giaccio R. Semi-dynamic Shortest Paths and Breadth-first Search in Digraphs // Proc. The 14-th Annual Symposium on Theoretical Aspects of Computer Science. 1997. pp. 33–46.

80. Frigioni D., Marchetti-Spaccamela A., Nanni U. Fully Dynamic Output Bounded Single Source Shortest Path Problem // Proc. ACM-SIAM Symposium on Discrete Algorithms. 1996.

81. Ramalingam G., Reps T. An Incremental Algorithm for a Generalization of the Shortest-Path Problem // Journal of Algorithms. 1996. Vol. 21. pp. 267–305.

82. Villamizar C. Convergence and restoration techniques for ISP interior routing // NANOG [Электронный ресурс], 2002. URL: http://www.nanog.org/mtg-0206/ppt/curtis.pdf (дата доступа 01.05.2015).

83. Labovitz C., Ahuja A., Bose A., Jahanian F. Delayed Internet Routing Convergence // IEEE/ACM Transactions on Networking (TON). 2001. Vol. 9. № 3. pp. 293-306.

84. Labovitz C., Ahuja A., Wattenhofer R., Venkatachary S. The impact of Internet policy and topology on delayed routing convergence // Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings (INFOCOM 2001). – IEEE, 2001. Vol. 1. pp. 537-546.

References

1. Goyal M., Soperi M., Baccelli E., Choudhury G., Shaikh A., Hosseini S. H., Trivedi K. Improving Convergence Speed and Scalability in OSPF: A Survey. *IEEE Communications Surveys & Tutorials*. 2012. no. 14(2). pp. 443-463. doi: 10.1109/SURV.2011.011411.00065. HAL Id: hal-00651596. Available at: https://hal.archives-ouvertes.fr/hal- 00651596 (accessed 01 May 2015).

2. Markopoulo A., Iannaccone G., Bhattacharya S., Chua C., Ganjali Y., Diot C. Characterization of failures in an operational IP backbone network. *IEEE/ACM Transactions on Networking*, 2008, vol. 16, no. 4.

3. Labovitz C., Ahuja A., Jahanian F. Experimental study of internet stability and backbone failures. *Proc. The 29-th International Symposium on Fault-Tolerant Computing*, Madison (WI, USA), 1999, pp. 278-285. doi: 10.1109/FTCS.1999.781062

4. Ganjali Y., Bhattacharyya S., Diot C. Limiting the impact of failures on network performance. *Sprint ATL Tech. Res. Rep., Tech. Rep. RR04-ATL-020666*, 2003. Available at: https://research.sprintlabs.com/publications/uploads/RR04-ATL-020666.pdf (accessed 01 May 2015).

5. Popovskii V. V., Volotka V. S. Metody analiza dinamicheskikh struktur telekommunikatsionnykh sistem [Methods of analysis of dynamic structures of telecommunication systems]. *Vostochno-Evropeiskii zhurnal peredovykh tekhnologii*, 2013, vol. 65, no. 5/2, pp. 18-22 (in Russian).

6. Popovskii V. V., Volotka V. S. Matematicheskoe modelirovanie nadezhnosti infokommunikatsionnykh sistem [Mathematical modelling of secure information and communication systems]. *Telekomunikacijni ta informacijni tehnologii'*, 2014, no. 3, pp. 5-9 (in Russian).

7. Popovskii V. V., Lemeshko A. V., Mel'nikova L. I., Andrushko D. V. Obzor i sravnitel'nyi analiz osnovnykh modelei i algoritmov mnogoputevoi marshrutizatsii v mul'tiservisnykh telekommunikatsionnykh setiakh [Basic models and algorithms of multipath routing for multi-service telecommunication networks]. *Prikladnaia radioelektronika*, 2005, vol. 4, no. 4, pp. 372-382. Available at: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (дата доступа 01.05.2015) (in Russian).

8. Lemeshko A. V., Evseeva O. Yu., Drobot O. A. The Method of Paths Independents Choice with Definition of their Quantity at the Solving of Multipath Routing Problem. *Praci UNDIRT*, 2006, vol. 48, no. 4, pp. 69-73. Available at: http://alem.ucoz.ua/_ld/0/14_Lemeshko_UNIIRT.pdf (accessed: 01 May 2015) (in Russian).

9. Lemeshko O. V., Kozlova H. V., Romanyuk A. O. A Mathematical Model of Fault-tolerant Routing, Presented Algebraic Equations of MPLS-Network State. *Systemy obrobky informacii'*, 2013, vol. 109, no. 2, pp. 217-220 (in Russian).

10. Popkov V. K. *Mathematical Models of Connection*. Novosibirsk, ICM&MG SB RAS Publ., 2006. 490 p. (in Russain).

11. Popkov V. K., Blukke V. P., Dvorkin A. B. Modeli analiza ustoichivosti i zhivuchesti informatsionnykh setei [Model analysis the sustainability and survivability of information networks]. *Problemy informatiki*, 2009, no. 4, pp. 63-78 (in Russian).

12. Sorokin A. A., Dmitriev V. N. Description of Communication Systems with Dynamic Network Topology by Means of Model "Flickering" Graph. *Vestnik of Astrakhan State Technical University. Series: Management, Computer science and Informatics*, 2009, no. 2. pp. 134-139 (in Russian).

13. Sorokin A. A., Dmitriev V. N., Tran Quoc Toan, Reznikov P. S. Evaluation of the Results of Using the RIP Protocol in Communication Systems with Dynamic Network Topology Using Simulation Method. *Vestnik of Astrakhan State Technical University. Series: Management, Computer science and Informatics*, 2014, no. 4, pp. 85-93 (in Russian).

14. Perepelkin D. A. Algoritm parnykh perestanovok marshrutov na baze protokola OSPF pri dinamicheskom otkaze uzlov i linii sviazi korporativnoi seti [The algorithm of pairwise permutations of routes for OSPF Protocol under condition dynamic failure of nodes and communication lines network]. *Vestnik Riazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*, 2014, vol. 47, no. 1, pp. 84-91 (in Russian).

15. Perepelkin D. A. Algoritm adaptivnoi uskorennoi marshrutizatsii na baze protokola IGRP pri dinamicheskom otkaze uzlov i linii sviazi korporativnoi seti [The algorithm is adaptive accelerated routing for IGRP Protocol under condition dynamic failure of nodes and communication lines network]. *Vestnik Riazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*, 2012, vol. 42, no. 4, pp. 33-38 (in Russian).

16. Perepelkin D. A. Dynamic Corporate Network Structure and Communication Links Loading Formation Based on Routes Pairs Permutations Data. *Informatsionnye tekhnologii*, 2014, no. 4, pp. 52-60 (in Russian).

17. Koriachko V. P., Perepelkin D. A. *Analiz i proektirovanie marshrutov peredachi dannykh v korporativnykh setiakh* [Analysis and design of routes of transmission of data in corporate networks]. Moscow, Goriachaia liniia – Telekom Publ., 2012. 236 p. (in Russian).

18. Meikshan V. I. Analysis of Equipment Faults Influence on Performance of Multiservice Network with Adaptive Routing. *Proceedings of the Russian higher school academy of sciences*. 2010, vol. 15, no 2, pp. 69-80 (in Russian).

19. Gorev P. G., Nazarov A. S., Pasechnikov I. I. Opredelenie sviaznosti v putevom prostranstve sostoianii telekommunikatsionnoi seti [The definition of connectivity in the route state-space telecommunication network]. *Tambov University reports. Series: Natural and Technical sciences*, 2012, vol. 17, no. 5, pp. 1360-1363 (in Russian).

20. Litvinov K. A., Pasechnikov I. I. Podkhody k resheniiu zadachi marshrutizatsii v sovremennykh telekommunikatsionnykh sistemakh [The routing problem in modern telecommunication systems]. *Tambov University reports. Series: Natural and Technical sciences*, 2013. vol. 18, no. 1, pp. 64-69 (in Russian).

21. Gromov Ju. Ju., Drachev V. O., Nabatov K. A., Ivanova O. G. *Sintez i analiz zhivuchesti setevyh sistem: monografija* [Synthesis and Analysis Net Systems Reliability]. Moscow, Mashinostroenie-1 Publ., 2007, 152 p. (in Russian).

22 Kovalkov D. A. Matematicheskie modeli otsenki nadezhnosti mul'tiservisnogo uzla dostupa [Mathematical model for reliability evaluation of multi-service access node network]. *Radio and telecommunication systems*, 2011, no. 2, pp. 64-71 (in Russian).

23. Gorbunov I. E. Metodologiia analiza i sinteza rekonfiguriruemykh topologii mobil'noi sviazi [The methodology of analysis and synthesis of reconfigurable topologies for mobile communication]. *Matematychni mashyny i systemy*, 2006, no. 2, pp. 48-59 (in Russian).

24. Egunov M. M., Shuvalov V. P. Analiz strukturnoi nadezhnosti transportnoi seti [Structural Reliability Analysis of Transport Network]. *Vestnik SibGUTY*, 2012, no. 1, pp. 54–60 (in Russian).

25. Makarenko S. I. Analiz vozdeistviia prednamerennykh pomekh na setevoi uroven' modeli vzaimodeistviia otkrytykh sistem i funktsionirovanie protokola marshrutizatsii otsenki sostoianiia kanala (OSPF) [Analysis of the Impact of Intentional Interference at the Network Level Model of Open Systems Interaction and Functioning of the Routing Protocol Assessment Channel (OSPF)]. *Informatsionnye tekhnologii modelirovaniia i upravleniia,* 2009, vol. 59, no. 7, pp. 956-961 (in Russian).

26. Makarenko S. I. Analiz vozdeistviia prednamerennykh pomekh na funktsionirovanie rasshirennogo protokola marshrutizatsii vnutrennego shliuza (EIGRP) [Analysis of Affecting Intended Interferences on the Operation of the Enhanced Interior Gateway Routing Protocol (EIGRP)]. *Informatsionnye tekhnologii modelirovaniia i upravleniia,* 2010, vol. 61, no. 2, pp. 223-229 (in Russian).

27. Bachinskii V. A., Giorgizova-Gai V. Sh. Vybor protokola dinamicheskoi marshrutizatsii v korporativnoi ip-seti [The choice of dynamic routing protocol in a corporate IP network]. *System Research & Information Technologies*, 2011, no. 1, pp. 99-110 (in Russian).

28. Sultanakhmetov D. Bystraia skhodimost' OSPF. Taimery protokola OSPF [Fast convergence OSPF. The OSPF timers]. *Network-Lab*, 09 January 2014. Available at: http://network-lab.ru/byistraya-shodimost-ospf-taymeryi-protokola-ospf/ (accessed 01 May 2015) (in Russian).

29. Moy J. T. *OSPF: Anatomy of an Internet Routing Protocol*. Addison-Wesley Professional, 1998. 338 p.

30. Tsegaye Y., Geberehana T. *OSPF Convergence Times. Master of Science Thesis in the Programme Networks and Distributed Systems*. Chalmers University of Technology. Göteborg (Sweden), 2012. 77 p. Available at: http://publications.lib.chalmers.se/records/fulltext/184363/184363.pdf (accessed 01 May 2015).

31. Goyal M., Xie W., Hosseini S. H., Vairavan K., Rohm D. Improving OSPF Dynamics on a Broadcast LAN. *Simulation*, 2006, vol. 82, no. 2, pp. 107-129. doi: 10.1177/0037549706065924

32. Moy J. RFC 2328. OSPF Version 2. *Network Working Group. Request for Comments*. Ascend Communications Inc, 1998.

33. Amir S., Biswajit N. Improving Network Convergence Time and Network Stability of an OSPF-Routed IP Network. *Lecture Notes in Computer Science*, 2005, Vol. 3462, pp 469-485. doi: 10.1007/11422778_38.

34. Choudhury G. RFC 4222. Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance. *Network Working Group, Request for Comments*. AT&T Publ., 2005.

35. *Cisco IOS Release 12.2(14)S. OSPF Update Packet-Pacing Configurable Timers.* Cisco, 2010. Available at: http://www.cisco.com/c/en/us/td/docs/ios/12_2s /feature/guide/fsospfct.html (accessed 01 May 2015).

36. Goyal M., Xie W., Soperi M., Hosseini S. H., Vairavan K. Scheduling routing table calculations to achieve fast convergence in OSPF protocol. *Proc. IEEE BROADNETS 2007*, 2007, pp. 863–872. doi: 10.1109/BROADNETS.2007.4550524.

37. Zaballos A., Seguí C. *Analysis and simulation of IGP routing protocols*. University Ramon Llull (La Salle Engineering), Barcelona (Spain). 2006. Available at: http://users.salleurl.edu/~zaballos/opnet/Trame.pdf (accessed 01 May 2015).

38. Alaettinoglu C., Jacobson V., Yu H. Towards milli-second IGP convergence. *IETF Draft*, 2000.

39. Fang W., Shanzhi C., Xin L., Yuhong L. A Route Flap Suppression Mechanism Based on Dynamic Timers in OSPF Network. *The 9-th International Conference for Young Computer Scientists,* IEEE, 2008.

40. Katz D., Ward D. RFC 5880. Bidirectional forwarding detection (BFD). *Internet Engineering Task Force, Request For Comments (Standards Track)*, 2010.

41. *Bidirectional Forwarding Detection for OSPF*. Cisco, 2005. 18 p. Available at: https://www.cisco.com/en/US/technologies/tk648/tk365/tk480/ technologies_white_paper0900aecd80244005.pdf (accessed 01 May 2015).

42. *Cisco IOS Software Releases 12.0 S. IP Event dampening*. Cisco, 2010. Available at: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/ s_ipevdp.html (accessed 01 May 2015).

43. Kolon M. C., Doyle J., Christensen S. *The Complete Reference Juniper Network Routers*. McGraw-Hill Osborne Media, 2002.

44. Baccelli E., Jacquet P., Nguyen D., Clausen T. RFC 5449. OSPF multipoint relay (MPR) extension for ad hoc networks. *Internet Engineering Task Force, Request for Comments (Experimental)*, LIX, Ecole Polytechnique, 2009.

45. Roy A., Chandra M. RFC 5820. Extensions to OSPF to support mobile ad hoc networking. *Internet Engineering Task Force, Request for Comments (Experimental)*, 2010.

46. Ogier R., Spagnolo P. RFC 5614. Mobile Ad-Hoc network MANET extension of OSPF using connected dominating set CDS flooding. *Internet Engineering Task Force, Request for Comments (Experimental)*, 2009.

47. Raj A., Ibe O. A Survey of IP and Multiprotocol Label Switching Fast Reroute Schemes. *Comput. Netw.*, 2007, vol. 51, no. 8, pp. 1882–1907.

48. Rosen E., Viswanathan A., Callon R., RFC 3031. Multiprotocol label switching architecture. *Internet Engineering Task Force, Request for Comments (Standards Track)*, 2001.

49. Davie B., Rekhter Y. *MPLS: Technology and Applications*. Morgan Kaufmann, 2000. 287 p.

50. Shaikh A., Wang D., Li G., Yates J., Kalmanek C. An efficient algorithm for OSPF subnet aggregation. *Proc. 11-th IEEE International Conference on Network Protocols (ICNP)*, 2003, pp. 200-209. doi: 10.1109/ICNP.2003.1249771

51. Coltun R., Ferguson D., Moy J., Lindem A. RFC 5340. OSPF for IPv6. *Internet Engineering Task Force, Request for Comments (Standards Track)*, 2001. Available at: http://www.rfc-editor.org/rfc/rfc5340.txt (accessed 01 May 2015).

52. Moy J., Pillay-Esnault P., Lindem A. RFC 3623. Graceful OSPF Restart. *Network Working Group, Request for Comments*, 2003. Available at: https://tools.ietf.org/html/rfc3623 (accessed 01 May 2015).

53. Li T., Cole B., Morton P., Li D. RFC 2281. Cisco Hot Standby Router Protocol (HSRP). *Network Working Group, Request for Comments (Informational)*, 1998. Available at: http://www.ietf.org/rfc/rfc2281.txt (accessed 01 May 2015).

54. Grebeshkov A.Iu. *Upravlenie setiami elektrosviazi po standartu TMN* [Network Management Using Concept of Telecommunication Management Network]. Moscow, Radio i sviaz' Publ., 2004. 156 p. (in Russian).

55. Kompella K., Rekhter Y. RFC 4203. OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS). *Internet Engineering Task Force, Request for Comments (Standards Track)*, 2005. Available at: https://www.ietf.org/rfc/rfc4203.txt (accessed 01 May 2015)

56. Pan P., Swallow G., Atlas A. RFC 4090. Fast Reroute Extensions to RSVP-TE for LSP tunnels. *Internet Engineering Task Force, Request for Comments (Standards Track)*, 2005.

57. Atlas A., Zinin A. RFC 5286. Basic specification for IP fast reroute: Loop-free Alternates. *Internet Engineering Task Force, Request for Comments (Standards Track)*, 2008.

58. Shand M., Bryant S. RFC 5714. IP fast reroute framework. *Internet Engineering Task Force, Request for Comments (Informational)*, 2010.

59. Shand M., Bryant S., Previdi S., IP fast reroute using not-via addresses. *Network Working Group, Internet-Draft (Experimental)*, 2010. Available at: https://tools.ietf.org/html/draft-ietf-rtgwg-ipfrr-notvia-addresses-06 (accessed 01 May 2015).

60. Atlas A. U-turn alternates for IP/LDP fast-reroute. *Network Working Group, Internet-Draft (Experimental)*, 2006. Available at: https://tools.ietf.org /html/draft-atlas-ip-local-protect-uturn-03 (accessed 01 May 2015).

61. Psenak P., Mirtorabi S., Roy A., Nguyen L., Pillay-Esnault P. RFC 4915. Multi-topology (MT) routing in OSPF. *Internet Engineering Task Force, Request For Comments (Standards Track)*, 2007.

62. Simpson W. RFC 1853. IP in IP tunneling. *Internet Engineering Task Force, Request For Comments (Informational)*, 1995.

63. Hanks S., Li T., Farinacci D., Traina P. RFC 1701. Generic routing encapsulation (GRE). *Internet Engineering Task Force, Request for Comments (Informational)*, 1994.

64. Ayari N., Barbaron D., Lefevre L., Primet P. Fault tolerance for highly available internet services: concepts, approaches, and issues. *IEEE Communication Surveys and Tutorials*, 2008, vol. 10, no. 2, pp. 34-46. doi: 10.1109/COMST.2008.4564478

65. Dilber M. N., Raza A. Analysis of successive Link Failures effect on RIP and OSPF Convergence time delay. *International Journal of Advances in Science and Technology*, 2014, pp. 42-48. Available at: http://sciencepublication.org/documents/sp/7.pdf (accessed 01 May 2015).

66. Zhao D., Hu X., Wu C. A Study on the Impact of Multiple Failures on OSPF Convergence. *International Journal of Hybrid Information Technology*. 2013. vol. 6. no. 3. pp. 75-74. Available at: http://www.sersc.org/journals/IJHIT/vol6_no3_2013/7.pdf (accessed 01 May 2015).

67. Sankar D., Lancaster D. Routing Protocol Convergence Comparison using Simulation and Real Equipment. *Advances in Communications, Computing, Networks and Security*, 2013, Vol. 10, pp. 186-194.

68. Antonova A. A. Performance evaluation in dynamic routing protocol streaming video. *Automation and Control in Technical Systems*, 2013, no. 4.2. Available at: http://auts.esrae.ru/7-151 (accessed: 02 May 2015). doi: 10.12731/2306-1561-2013-4-36

69. Pun H. *Convergence Behavior of RIP and OSPF Network Protocols*. Ph.D. Thesis. B.A.Sc., University of British Columbia, 2001. 59 p. Available at: http://www2.ensc.sfu.ca/~ljilja/cnl/pdf/hubert.pdf (accessed: 02 May 2015).

70. Huang S., Kitayama K., Cugini F., Paolucci F., Giorgetti A., Valcarenghi L., Castoldi P. An Experimental Analysis on OSPF-TE Convergence Time. *Asia Pacific Optical Communications – International Society for Optics and Photonics*, 2008, vol. 7137. doi:10.1117/12.803224

71. Makarenko S. I., Mikhailov R. L., Novikov E. A. Issledovanie kanal'nykh i setevykh parametrov kanala sviazi v usloviiakh dinamicheski izmeniaiushcheisia signal'no–pomekhovoi obstanovki [The Research of Data Link Layer and Network Layer Parameters of Communication Channel in the Conditions Dynamic Vary of the Signal and Noise Situation]. *Journal of Radio Electronics*, 2014, no. 10. Available at: http://jre.cplire.ru/jre/oct14/3/text.pdf (accessed 3 May 2015) (in Russian).

72. Goyal M., Ramakrishnan K. K., Feng W. Achieving Faster Failure Detection in OSPF Networks. *Proc. IEEE International Conference on Communications (ICC-2003)*, 2003, vol. 1, pp. 296-300. doi: 10.1109/ICC.2003.1204188

73. Basu A., Riecke J. Stability issues in OSPF routing. *ACM SIGCOMM Computer Communication Review*, 2001, vol. 31, no. 4, pp. 225-236.

74. Choudhury G., Ash G., Manral V., Maunder A., Sapozhnikova V., *Prioritized treatment of specific OSPF packets and congestion avoidance: algorithms and simulations*. Technical Report, AT&T Publ., 2003.

75. Liu Y., Zhao X., Nam K., Wang L., Zhang B. Incremental For warding Table Aggregation. *GLOBECOM 2010*, Miami, Florida, USA, 2010. pp. 1-6.

76. Tsvetcov K. U., Makarenko S. I., Mikhailov R. L. Forming of Reserve Paths Based on Dijkstra's Algorithm in the Aim of the Enhancement of the Stability of Telecommunication Networks. *Informatsionno-upravliaiushchie sistemy*, vol. 69, no. 2, 2014, pp. 71-78 (in Russian).

77. Pu J., Manning E., Shoja G. C., Routing Reliability Analysis of Partially Disjoint Paths. *Proc. IEEE Conference on Communications, Computers, and Signal Processing*, Victoria (BC, Canada), 2001, vol. 1, pp. 79-82.

78. McQuillan J., Richer I., Rosen E. The New Routing Algorithm for the ARPANET. *IEEE Transactions on Communications*, vol. 28, no. 5, 1980.

79. Franciosa P., Frigioni D., Giaccio R. Semi-dynamic Shortest Paths and Breadth-first Search in Digraphs. *Proc. The 14-th Annual Symposium on Theoretical Aspects of Computer Science*, 1997, pp. 33–46.

80. Frigioni D., Marchetti-Spaccamela A., Nanni U. Fully Dynamic Output Bounded Single Source Shortest Path Problem. *Proc. ACM-SIAM Symposium on Discrete Algorithms*, 1996.

81. Ramalingam G., Reps T. An Incremental Algorithm for a Generalization of the Shortest-Path Problem. *Journal of Algorithms*, 1996, vol. 21, pp. 267–305.

82. Villamizar C. Convergence and restoration techniques for ISP interior routing. *NANOG* [Online], 2002. Available at: http://www.nanog.org/mtg-0206/ppt/curtis.pdf (accessed 01 May 2015).

83. Labovitz C., Ahuja A., Bose A., Jahanian F. Delayed Internet routing convergence. *IEEE/ACM Transactions on Networking (TON)*, 2001, vol. 9, no. 3, pp. 293-306.

84. Labovitz C., Ahuja A., Wattenhofer R., Venkatachary S. The impact of Internet policy and topology on delayed routing convergence. *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings (INFOCOM 2001)*, IEEE, 2001, vol. 1, pp. 537-546.

Статья поступила 22 мая 2015 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей и систем связи к преднамеренным деструктивным воздействиям; радиоэлектронная борьба; информационное противоборство. E–mail: mak-serg@yandex.ru

Адрес: Россия, 197198, г. Санкт-Петербург, ул. Ждановская д. 13.

Convergence Time of IGP Routing Protocol

Makarenko S. I.

Statement of the problem. *Network* communications *are augment structural complexity, so ensuring the sustainability of the networks provided that the failure of individual channels and nodes becomes relevant. Review of failure statistics showed that 70% of failures in networks occurs due to deterioration of telecommunications equipment, 20% - because of incorrect maintenance operations, 17% - due to software errors. Routing protocols should ensure correct handling of failures in the network. They must do it with minimum time spent.* ***Purpose*** *– research of convergence time of the networks and estimate impact of time parameters of routing protocols, the complexity of the network topology, channel capacity and network load to convergence time of the networks.* ***Methods****. Author study convergence time in terms of publishing papers in this subject area. We review failure statistics and analyses of protocol insidedomain routing in the first part of the paper. The results of the analysis have shown that the best results in terms of convergence time of the network protocols based on the analysis of the channel state. In the second part of the article we have analyzed temporal parameters of the routing Protocol and the principles of operation of this Protocol which affect the convergence time of failure in the network. In the third part we have reviewed and classified the main technological solutions are used by manufacturers of telecommunications equipment to reduce the time of convergence. In the fourth part of this paper we reviewed the results of studies in the convergence time of the network for different routing protocols and different configurations time parameters. We compared the values of convergence time of the network in the simulation network in OPNET environment with the values of convergence time in experiments using telecommunication equipment. In the fifth part of the article we analyze the directions of improvement of routing protocols, in the part which refers to the reduced time of convergence, based on fresh research papers.* ***Innovation. G****eneralized analysis of the functioning of routing protocols and the influence of temporal parameters of these protocols on the convergence time of the network are the elements of novelty. Theoretical generalization of the directions of the improvement of routing protocols, increasing the resilience of the network to failures and reducing convergence time are the elements of novelty.* ***The result and practical relevance.*** *The material of the article can be used to justify new algorithms for traffic routing in networks with failures. Routing protocols OSPF, OSPF-TE, IS-IS, IGRP, EIGRP can be improved by the analysis of perspective directions. Some solutions are discussed in the paper can be used to develop routing protocols for MANET mobile networks and networks based on Mesh technology.*

Key words: *routing, IGP, convergence time, the network failure, OSPF, OSPF-TE, IS-IS, IGRP, EIGRP, MANET*

Information about Author

Makarenko Sergey Ivanovich – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. A. F. Mozhaisky Military Space Academy. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. Тел.: +7 981 820 49 90. E–mail: mak-serg@yandex.ru

Address: Russia, 197198, Saint-Petersburg, Zjdanovskaya ulica, 13.