УДК 621. 395.7

Резервирование и восстановление в телекоммуникационных сетях

М.М. Егунов, В.П. Шувалов

Представлен обзор основных методов резервирования, обеспечивающих повышение структурной надёжности телекоммуникационных сетей. Описаны их достоинства и недостатки. Дана классификация способов резервирования (защитного переключения) и восстановления (перемаршрутизации). Описан подход к определению требуемого значения коэффициента готовности исходя из “степени воздействия отказа”, который зависит от времени восстановления, количества потерянных пакетов вследствие отказа узлов и линий связи, а также экономических показателей.

Ключевые слова: структурная надежность, резервный путь, резервирование, восстановление, коэффициент готовности, класс готовности, время восстановления, методы защиты, п-циклы, степень воздействия отказа.

Процесс восстановления связи между двумя конечными узлами может происходить путём перенаправления трафика на заранее подготовленный до установления соединения резервный путь (proactive). Этот метод принято называть резервированием (reservation) или защитой переключением. Другим вариантом восстановления соединения является поиск нового пути (перемаршрутизация) после возникновения отказа. Этот метод принято называть восстановлением (restoration) или динамическим (reactive) восстановлением. Последний термин является, на наш взгляд, более предпочтительным, так как переход на заранее подготовленный резервный путь тоже является восстановлением соединения. Однако, для сокращения, вместо термина «динамическое восстановление» будем пользоваться в дальнейшем термином «восстановление». Кстати, в англоязычной литературе именно этот термин (restoration) и используется.

Достоинством метода резервирования является быстрое восстановление связи, недостатком – необходимость в дополнительной, иногда очень существенной, пропускной способности. Метод восстановления требует больших затрат времени на восстановление связи, кроме того, возникает риск нестабильности сети, особенно в случае частых самоустраняющихся сбоев [1]. Достоинством метода восстановления является лучшее использование пропускной способности сети связи. Описание и анализ методов резервирования можно, например, найти в работах [2 – 7], методов восстановления – в [8 – 12], а также монографиях [13 – 14].

Резервирование и восстановление позволяют обеспечить требуемый потребителем показатель готовности соединения или показатель готовности услуги.

Готовность – это вероятность того, что соединение будет обеспечено в любой случайный момент. Это важнейшая метрика, отражающая структурную надёжность сети.

При выборе сетевого сервиса готовность услуги является одной из многих тесно связанных метрик, иногда даже более важных, чем другие QoS параметры, такие, как задержка, джиттер, потеря пакетов.

Анализ рынка телекоммуникационных услуг показывает, что 50 % пользователей услуг ожидают, по крайней мере, 99.9 % доступности сервиса [15]. Финансовые потери в результате отсутствия связи на бирже в течение 1 минуты чреваты убытками порядка $ 110 000 [15]. Поэтому для бизнес-клиентов требуется обеспечить коэффициент готовности 0.999999, что

соответствует длительности простоя в год 0.53 минуты или шестому классу доступности (таблица 1).

Таблица 1. – Классы готовности систем

Тип системы	**Недоступность (мин/год)**	**Доступность**	**Класс готовности**
Необслуживаемые	50 000	90 %	1
Обслуживаемые	5 000	99 %	2
Хорошо обслуживаемые	500	99.9 %	3
Отказоустойчивые	50	99.99 %	4
Высокая готовность	5	99.999 %	5
Очень высокая готовность	.5	99.9999 %	6
Сверхвысокая готовность	.05	99.99999 %	7

Заметим, что более высокая готовность требует более высоких затрат со стороны оператора, что сказывается на цене услуги. А так как разные пользователи имеют различную чувствительность к доступности сервиса, то пользователи с лимитированным бюджетом должны иметь удовлетворяющий их по цене уровень доступности. Отсюда возникла идея обеспечения эластичного (гибкого) доступа к сервису [16], которая предполагает, в частности, разные варианты резервирования в зависимости от требований потребителя к коэффициенту готовности. Более того, сопоставляя финансовые потери при отказах и затраты на обеспечение $K_Г$, можно найти наиболее приемлемое, с точки зрения потребителя, значение $K_Г$ [17,18].

Надёжность функционирования сетевой инфраструктуры обеспечивается путём использования алгоритмов резервирования и восстановления связи между сетевыми узлами и средств повышения надёжности самих узлов, в первую очередь маршрутизаторов и коммутаторов. Сегодня все серьёзные технические решения требуют как минимум двух модулей управления, характеризуются избыточностью различных подсистем с возможностью их быстрой замены в «горячем» режиме [19].

Для определения степени защиты, требуемой для данного участка сети, необходимо учитывать вероятность отказа участка сети и предполагаемые воздействия на трафик (в понятиях времени восстановления, вероятности потери пакетов) [12].

Значение вероятности отказа заданного участка сети (то есть области защиты) можно определить на основании доступной информации о характере происходящих отказов. Начальное значение вероятности отказа может быть уточнено на основе фактической статистики отказов.

Если вероятность отказа известна, необходимо рассмотреть, как отказ влияет на трафик в сети, то есть, определить «степень воздействия отказа». Критическим аспектом для оценки воздействия отказа является гарантируемое качество обслуживания *(QoS)* трафика, которое определяется двумя компонентами: временем восстановления и количеством потерянных пакетов.

Время восстановления T_B определяется циклом восстановления пути. Заметим, что этот цикл можно задать следующими составляющими:

1) временем обнаружения отказа T_1;
2) временем удержания (в случае необходимости) T_2;

3) временем уведомления (т.е. посылки сообщения узлу, ответственному за переключение) T_3;

4) временем для резервирования маршрута и сигнализации T_4;

5) временем для переключения трафика T_5 с активного пути на резервный путь.

Количество потерянных пакетов $N_{ПП}$ пропорционально времени восстановления T_B и скорости передачи пакетов R, т.е. $N_{ПП} = RT_B$.

Сокращение времени обнаружения отказа и времени переключения зависит от используемой технологии восстановления. Кроме того, время установления резервных путей (при обнаружении отказа) зависит от метода маршрутизации и используемых методов сигнализации.

Сокращение времени уведомления T_3 – вероятно, основной аспект при проектировании методов защиты для сети. Время уведомления зависит от времени распространения между узлами сигнала об отказе T_p и от расстояния $D(i,a)$, которое может быть определено как количество участков сети (рёбер) между узлом, обнаружившим отказ (узел a), и узлом, ответственным за переключение (узел i).

$$T_{УВ} = T_P \cdot D(i,a).$$

Так как время распространения сигнала об отказе зависит от характера среды распространения сигнала, то снижение $T_{УВ}$ может быть достигнуто уменьшением расстояния $(D(i,a))$. Местное (local) резервирование обеспечивает оптимальное значение $(D(i,a) = 0)$. Главная проблема состоит в том, что расстояние $D(i,a)$ неизвестно заранее, потому что неизвестно, какое ребро пути выйдет из строя. Однако знание вероятностей отказа участков пути P_i можно использовать, чтобы оценить вероятности появления тех или иных значений $D(i, a)$ и вычислить среднее значение $D(i,a)$

$$D(i,a) = \sum_i P_i D(i,a).$$

При проектировании сети необходимо стремиться уменьшить как вероятность отказа, так и воздействие отказа. Это непростая задача, поскольку существует взаимная связь между снижением степени воздействия отказа и снижением вероятности отказа.

Современные телекоммуникационные сети – это сети, обладающие огромной пропускной способностью и использующие на физическом уровне, как правило, волоконно-оптические линии связи. Поэтому задача обеспечения структурной надёжности таких сетей является чрезвычайно актуальной [20].

Резервирование и восстановление являются двумя основными подходами, обеспечивающими структурную надёжность телекоммуникационных сетей при выходе из строя узлов и линий связи.

Перечислим основные требования к методам обеспечения надежности сетей. Помимо требований к экономии пропускной способности, здесь следует учесть ограничения на компьютерные ресурсы, скорость замещения, сложность предлагаемых методов и масштабируемость.

Заметим, что задача оптимизации какого-либо из показателей при наличии ограничений является в большинстве случаев сложной задачей (NP-complet). Для её решения могут использоваться различные методы. А именно, метод неопределённых множителей Лагранжа [21], методы линейного и нелинейного целочисленного линейного программирования [21 – 24] и др. Однако чаще всего для решения поставленной задачи используют эвристические методы (см., например, [25]).

Рассмотрим классические модели резервирования сетей связи (рис.1) и дадим их краткую характеристику. Физическая топология сети состоит из узлов, соединённых линиями связи (каналами связи, звеньями). При рассмотрении процесса передачи от источника к получате-

лю вводится понятие «путь». Различают первичные (рабочие) пути и пути резервные. Отрезок пути, состоящий из нескольких звеньев, принято называть «сегментом». Понятие «сегмента» можно рассматривать как обобщение понятий «рабочий путь» и «звено».

На рис.1а представлена модель защиты звена. Здесь каждое звено защищается в индивидуальном порядке (локальная защита). Этот метод обладает высокой вычислительной эффективностью, обеспечивает быструю перемаршрутизацию, прост и масштабируем, но нуждается в больших сетевых ресурсах.

Защита пути (рис.1в) осуществляется из конца в конец, т.е. от источника до получателя (иногда такую защиту называют глобальной). Здесь сетевые ресурсы используются более экономно, но вычисление пути из конца в конец является более сложной задачей. Различают два варианта такой защиты: а) альтернативный путь, использующий одно или несколько звеньев рабочего пути; б) альтернативный путь, ни в одном из звеньев не совпадающий с первичным путём. Второй вариант представляет интерес для случая, когда сбои могут произойти в любом из звеньев первичного пути (тогда для каждого из случаев отказа в первом варианте пришлось бы искать свой альтернативный путь). Восстановление при втором варианте может быть начато немедленно после обнаружения сбоя любого звена первичного пути без ожидания конкретизации звена, вышедшего из строя.

На рис.1с и рис.1д представлены модели защиты сегмента (участка из нескольких звеньев). Модель на рис. 1д отличается тем, что здесь выполнена защита с «наложением», это позволяет обеспечить обход вышедших из строя узлов (кроме узлов источника и получателя).

Хорошо известный случай кольцевой защиты, так называемая защита на основе П-циклов (P-cycle), представлен на рис.1а. Данный метод защиты относится к сегментным. Суть механизма резервирования на основе П-циклов заключается в выделении на высокосвязной топологической структуре замкнутого контура или цикла с предварительно рассчитанной резервной пропускной способностью, которая будет использоваться в случае возникновения отказа в сети связи. Для организации П-цикла в сети необходимо найти функционально замкнутый контур, который должен проходить через возможно большее количество узлов и иметь минимальную протяжённость. Использование при организации резервирования механизма П-циклов требует около 30 % дополнительной пропускной способности, что значительно меньше в сравнении со значениями, необходимыми при кольцевом резервировании [26 – 28].

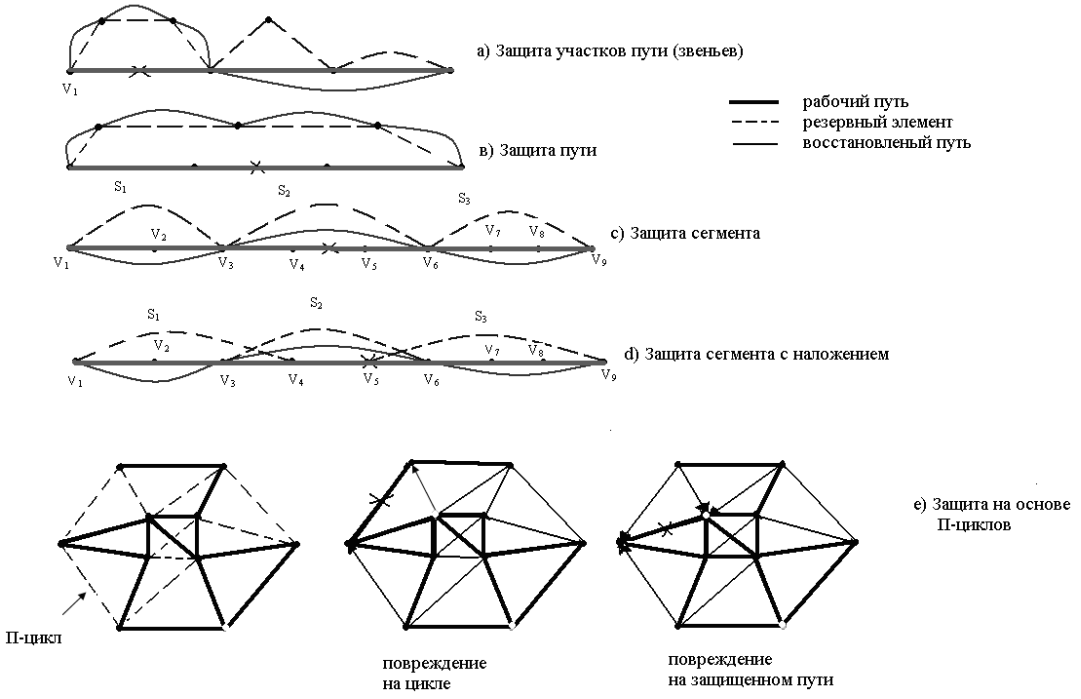

Рис. 1. – Классические модели резервирования

На примере моделей, представленных на рис. 1, мы рассмотрели только подходы к выбору области защиты (или масштаба защиты). Ниже мы остановимся на известных методах использования ресурсов пропускной способности, таких как 1+1, 1:1, *M:N,* которые могут использоваться как в вариантах защиты пути, так и звена или сегмента.

Защита пути 1+1. Данные передаются одновременно по рабочему и резервному пути. На приёме выделяется лучший сигнал. Рабочий и резервный пути разделены.

Защита звена 1+1. Принцип действия такой же, как в случае защиты пути, но обеспечивается обход только одиночного сбойного звена или узла, а не всего пути.

Защита звена 1:1. До отказа данные посылаются только по рабочему пути. Второстепенный трафик может транслироваться по резервному пути. В случае отказа на рабочем звене прекращается передача второстепенного трафика, и данные передаются по резервному звену, который становится рабочим.

В случае устранения отказа рабочего пути возможны следующие варианты:

1) трафик с резервного пути перебрасывается обратно на рабочий путь;

2) трафик после устранения отказа остаётся на резервном пути, в то время как рабочий путь выполняет функцию резервного.

Достоинством первого варианта является использование приоритетным трафиком более надёжного пути, каковым обычно является рабочий путь. Недостатком – необходимость переключения, которое выполняется устройством, имеющим $K_Г$<1.

Защита пути 1:1. Принцип действия такой же, как в случае защиты звена 1:1, но здесь обеспечивается обход всего повреждённого пути. В вариантах 1+1 и 1:1 использовались выделенные ресурсы пропускной способности, в качестве которых можно рассматривать в том числе и волокно, и оптический канал.

В ряде случаев используется так называемая групповая (Shared) защита или защита *M:N,* которая является обобщением защиты 1:1, *(M=1, N=1).*

Защита звена *M:N*. Рабочий и резервный пути организованы до отказа (*N* рабочих, *M* резервных, *N*≥*M*). В случае отказа на звене, данные переключаются на резервное звено, но если повреждено более чем *M* рабочих звеньев, второстепенный трафик теряется. Наиболее часто используемый вариант *M:N* соответствует случаю, когда *M=1 (1:N)*. Применительно к MPLS защита звена *M:N* имеет название «быстрая перемаршрутизация» (fast reroute) [29].

Защита пути *M:N*. Принцип действия такой же, как и в случае защиты звена, но здесь обеспечивается обход всего пути. Этот метод резервирования наиболее востребован вследствие своей низкой стоимости и гибкости. Однако он достаточно сложен в оптимизации, особенно в случае, если используются механизмы, учитывающие приоритеты [30].

Рассмотренные выше процедуры резервирования могут использоваться совместно с процедурами восстановления. Так, например, можно разделить весь трафик на несколько типов в соответствии с их приоритетами и, соответственно, разной чувствительностью к времени восстановления соединения. Для наиболее чувствительного к задержкам трафика можно применить защиту 1+1 или 1:1, для менее чувствительных – алгоритмы восстановления. Другой вариант совмещения – перейти при одновременном сбое на резервном и первичном (рабочем) каналах в схеме 1+1 на использование одного из возможных алгоритмов восстановления. Разумеется, этими двумя вариантами перечень возможных подходов к проблеме совместного использования процедур резервирования и восстановления не исчерпывается.

Обобщенная характеристика методов защиты от отказов представлена в табл. 2.

Таблица 2. – Опции защиты

Методы защиты		
Защитное переключение (резервирование)	Восстановление (перемаршрутизация)	
Выделение ресурсов		
Предварительное	По требованию	
Использование ресурсов		
Выделенные	Общие	Второстепенного трафика
Создание пути		
Предварительное	В соответствии с требуемым качеством	По требованию
Масштаб защиты		
Глобальная (пути)	Локальная (звена)	Сегмента
Защитное переключение		
Автоматическое (внутренний сигнал)	Внешние команды	

Если первая часть работы в основном посвящена методам резервирования, то во второй части предполагается рассмотреть вопросы перемаршрутизации после возникновения отказа и вопросы совместного использования методов резервирования и восстановления.

Литература

1. *Bircan G., Cannington J., Ortynski E.A., and Spiride G.* «Design strategies for meeting unavailability targets using dedicated protection in DWDM networks». IEEE/OSA J. Lightwave Technolody, vol. 25, no.5, pp.1120 – 1129, May 2007.

2. *Шувалов В.П., Тимченко С.В.* Методы резервирования и восстановления в телекоммуникационных сетях. Межвузовский тематический сборник научных трудов. – Омск, 2009. – С. 40-43.

3. *Егунов М.М., Минина Е.А., Шувалов В.П., Трибунский Д.С.* Структурная надёжность сетей связи. Учебное пособие.- Екатеринбург, УрТИСИ, 2011. – 51 с.

4. Network reliability and availability// Электронный ресурс.
WWW. network – protection / network – reliability – and – availability. 2010.

5. ГОСТ 53111 – 2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. Стандартформ. 2008.

6. *Калимулина Э.Ю.* Моделирование и анализ надёжности корпоративной сети. // Стандарты и качество. – 2008, № 8. – С. 96-112.

7. *Ромашкова О.Н., Иванов П.А., Васюк Д.С.* Анализ отказоустойчивости плоскости управления. Спецификации Generalized Multi-Protocol Label Switching. ИКСЗТ, 2010, №5. – С. 14-17

8. *Поповский В.В., Лемешко А.В., Мельникова Л.Н., Андрушко Д.В.* Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника.–2005.-Том 4.– Вып. № 4. – С. 372-382.

9. *Gao D. and Zhang H.* «Routing pre-configuration for fast and scalable path restoration in DWDM networks». Photonic Network Commun., vol. 12, no 3, pp. 321-327, Dec. 2006.
10. *Iraschko R. and Grover W.* «A highly efficient path restoration protocol for management of optical network transport integrity». IEEE J. Sel. Areas Commun, vol. 18, no 5, pp. 779-794, May 2000.
11. *Norden S., Buddhikot M., Waldvogel M. and Suri S.* «Routing bandwidth-guaranteed paths with restoration in label switched networks». Comput. Netw, vol. 46, no. 2, pp. 197-218, 2004.
12. *Ananya Das, Charles Martel, Biswanath Mukherjee, and Smita Rai.* «New Approach to Reliable Multipath Provisioning.» J. Opt. Commun. Netw, vol. 3, no 1, January 2011.
13. *Vasseur J., Pickavet M., Demester P.* «Network Recovery. Protection and Restoration of Optical, SONET-SDN, IP, and MPLS». Morgan Kaufman Publishers. 2004. – 521 p.
14. *Будылдина Н.В., Трибунский Д.С., Шувалов В.П.* «Оптимизация сетей с многопротокольной коммутацией по меткам». – М.: Горячая линия – Телеком, 2010. – 144 с.
15. *G. Holland.* «Carrier class metro networking», Riverstone Networks, Technology white paper no.135, july 2002.
16. LYNX Photonic Network Inc, Achieving high avalibility protection systems. White paper, 2005. Электронный ресурс.
http: // www. Lynx-networks.com/content.asp?pade=whitepapers&id=8.
17. *Lei Song, Beswenath Mukherjee.* «On the study of Multiple Backups and Primary-Backup Link shuring for Dynamic Service Pronsioning in Survivable WDM Mesh Networks». IEEE Journal on selected Areas in Communicatios, vol. 26, no 6. August 2008.
18. Теория надёжности. Показатели экономической эффективности промышленных объектов. Экономические критерии. Оптимизации технических решений. Электронный ресурс. http// reliability – theory.ru/topics/ t 6 r 2 part 1. html.
19. *Половко А.М., Гуров С.В.* Основы теории надёжности. БХВ – Петербург, 2008. – 560 с.
20. *Mukherjee B.* «Optical WDM Networks». Springer. 2006. – 956 p.
21. *Яковлев А.В.* Надёжность информационных систем. – Муром. – 2004. – 63 с.
22. *Хемди А. Таха.* Введение в исследование операций, 7-е издание: Перев. с англ. – М.: Издательский дом «Вильнюс», 2005. – 901 с.
23. *Гончаров В.А.* Методы оптимизации. – М.: «Высшее образование», 2009. – 191 с.
24. *Вентцель Е.С.* Исследование операций. Задачи, принципы, методология. – М.: «Изд. КноРус», 2010. – 191 с.
25. *Pin Han Ho, Topolcoi Janos and over.* «Diverse Routing for Shared Protection in Surviable Optical Networks». ICC, 2003.
26. *Семёнов Ю.А.* Алгоритмы телекоммуникационных сетей: учебное пособие. Часть 1. – М.: Университет информационных технологий; БИНОМ. Лаборатория знаний, 2007. – 637 с.
27. *Комарницкий Э.И.* Надёжность волоконно-оптических сетей связи и оперативное устранение аварий // LIGHTWAVE Russian Edition, 2005, № 4. – С. 37-43.
28. *Kodian A., Grover W.* «Failure. – Independent Path-Protecting p-Cycles: Efficient and Simple Fully Preconnected Optical-Path Protection» // Journal of Lightwave Technology, vol. 23, no 10. – 2005.
29. *Cholde P., Jojszyk A.* «Reliability Assessment of p-Cycles» // IEEE Global Telecommunication Conference (GlobeCom 2005), st. Lonis, November-December 2005.
30. *Pan P., Swallow G. and Atlas*. «Fast Reroute Extensions to RSVP-TE for LSP Tunnels», RFC 4090 (Propoused Standart), Internet Engineering Task Force, May 2005.
31. *Fawaz W., Martignon F., Chen K., Pujolle.* «Novel Protection Scheme for Quality of Service Aware WDM Networks», ICC, 2005.

Статья поступила в редакцию 20.03.2012