УДК 654.078

[1]С.В.Самоделкина, [2]Г.Г.Таткеева, [2]Г.Ш.Оразгалиев, [2]В.И.Эйрих,
[2]А.Д.Мехтиев, [2]В.В.Югай

[1]Алматинский университет энергетики и связи;
[2]Карагандинский государственный технический университет
(E–mail:barton.kz@mail.ru)

Влияние отказов на процессы управления телекоммуникационной системой и передачи информации в ней

В статье рассматриваются вопросы управления устранением последствий отказов и их локализация. Показано влияние отказов на процесс передачи и распределения информации, на надежность функционирования и методы восстановления системы связи. Приведены методики обеспечения устойчивости узлов к сбоям. Предложена классификация сбоев, алгоритмы восстановления нормального функционирования системы, которые зависят от источников проблемы. Описана стратегия для обеспечения устойчивости сети связи.

Ключевые слова: надежность сетей связи, локализация отказов, классификация сбоев, восстановление системы, отказоустойчивость сети, процесс управления.

За последние 10–15 лет произошли существенные изменения в инфраструктуре телекоммуникационных систем и инфокоммуникационных технологий. В современных условиях конвергенции информационных технологий и средств связи корпоративные сети становятся более сложными, как по архитектуре, так и по предоставляемым услугам.

Учитывая необходимость повышения предоставления услуг, новые приложения — а это мультимедийные приложения, а также приложения, адаптируемые к требованиям пользователя, — становятся неотъемлемой частью всех процессов в работе телекоммуникационных систем. В этой новой среде функция управления технологиями перемещается из парадигмы сетевых функций в парадигму функций приложений. Несмотря на такой сдвиг, новый фокус повышает значимость сети, потому что качество и надежность функционирования сети в конвергентной среде с возможностью круглосуточного доступа непосредственно связаны с качеством передачи (QoS).

Поставщикам услуг необходимо поддерживать непрерывность услуг и соответствующее качество передачи для выполнения строгих обязательств перед пользователями. Надежность обслуживания должна быть предусмотрена на уровне каждого элемента сетевого проекта. Это необходимо для защиты услуг от сбоев, обусловленных неисправностью аппаратных средств, IP-маршрутизации, или канальными отказами, а также для защиты от злонамеренных DoS-атак (отказ от обслуживания), при модификации программного обеспечения или от ошибок конфигурирования маршрутизатора. От поставщиков услуг требуется обеспечить минимизацию дорогостоящего времени простоя систем путем быстрого и эффективного диагностирования и устранения проблем.

В современных цифровых сетях для управления активно используется мониторинг. Система мониторинга предназначена для реализации принципов управления эксплуатационной работой отдельной сети связи за счет автоматизации функций контроля и мониторинга работоспособности оборудования, состояния связи между объектами, качества передачи информации между абонентами, а также функций управления оборудованием и ресурсами сети.

Получение полной и достоверной информации о состоянии объектов мониторинга сети связи всегда было актуальной задачей. Такую возможность можно получить только при использовании надежной связи и оборудования, что не всегда удается. Если произойдет отказ оборудования или прерывание связи на участке сети в направлении от объекта мониторинга к серверу мониторинга, в полученных данных появляются «провалы», вызванные неполучением откликов на запрос состояния определенных ресурсов удаленных объектов. В результате, в случае прерывания связи с объектом, администратор сети может сделать неправильные выводы о качестве работы сети [1].

Решения сетевого управления принимаются на основе информации, полученной из систем мониторинга в сети (например, с помощью Simple Network Management Protocol [SNMP]). Однако для того чтобы сделать независимое решение о характере проблем и реакции на них, нужно использовать более широкий спектр информации, чем необходимые данные для разрешения проблемы сети связи.

Помимо традиционной информации мониторинга сети иногда может быть использована внешняя информация о ситуации.

На гарантированное предоставление услуг «всегда на связи» влияют три основные операционные области:

– уменьшение числа сетевых отказов;

– своевременная локализация отказов;

– отработанные процедуры эксплуатации технического обслуживания.

Диагностика отказов является центральным аспектом управления отказами в сетях связи. Так как неисправности неизбежны в системах связи, их быстрое обнаружение и изоляция играют важную роль для прочности, надежности и доступности системы. В больших и сложных сетях связи автоматизация диагностики имеет решающее значение при работе оператора связи с приложениями по управлению сетью и услугами [2]. Для этого используются инструментальные средства OAM (Operations Administration Maintenance — эксплуатация, управление и техническое обслуживание), которые позволяют устанавливать упреждающие политики контроля, эффективно выполнять конфигурирование услуг, применять политики верификации и расширенные процедуры локализации отказов для обеспечения быстрого восстановления работы системы связи.

Правильная услуга предоставляется, когда служба реализует функции системы. Сбой системы является событием, которое происходит, когда предоставляемая услуга отклоняется от правильного обслуживания и это не соответствует спецификации. Отказ является переходом от правильной услуги к неправильному обслуживанию, т.е. не выполняется функция системы связи.

Сбой происходит, когда ошибка достигает интерфейса сервиса и видоизменяет службы. Система состоит из множества взаимодействующих компонентов, поэтому состояние системы связи является множество состояний его компонентов. Неисправность первоначально вызывает ошибку в состоянии одного (или более) компонентов, но сбой системы не произойдет, пока ошибка не достигнет интерфейса системы. Ошибка считается обнаруженной, если ее присутствие в системе указывается в сообщении об ошибке или при наличии сигнала рассогласования, который появляется в системе. Ошибки, которые присутствуют, но не обнаружены, являются скрытыми [3].

Анализ процессов функционирования сетей связи позволяет произвести оценку влияния отказов на процесс передачи и распределения информации, на надежность функционирования сетей связи.

К числу основных факторов отказов в сетях связи относятся следующие:

– отказы и восстановления технических средств;

– естественные помехи;

– искусственные помехи;

– разрушающие искусственные воздействия;

– ошибки программного обеспечения СС;

– отказы, вызванные деятельностью человека;

– отказы, вызванные природными явлениями.

Классификация сбоев и понимания их природы является существенным, если необходимо разработать систему, которая способна функционировать, несмотря на сбои и отказы в сети связи.

Основные направления для правильной и точной классификации сбоев и дальнейшего восстановления системы следующие:

– классификация отказов должна быть независима от какой-либо конкретной системы, т.е., применима к любой системе;

– классификация отказов должна быть как можно более подробной; единственное ограничение в подробности – разделения в значимых классах, которые могут быть использованы для выявления надлежащего набора методов по обнаружению сбоев, характерных для данного класса;

– обработка отказов является шагом, который следует после их обнаружения, а также последствий сбоев, которые следует рассматривать в качестве второго этапа, так как они могут потребовать дополнительной детализации и анализа [4].

Процесс восстановления включает в себя четыре основные группы: модель сбоев, реакцию системы на них, функциональный цикл работы и цикл восстановления.

Модель сбоев — это основа для разработки алгоритмов восстановления системы. Она базируется на спецификации системы определять ее устойчивость к различным видам отказов. В общем слу-

чае важны следующие характеристики: длительность сбоев, их симптомы и источники, степень поражения системы, профиль ожидаемых сбоев.

По длительности сбои можно разделить на три категории:

– постоянные — устраняются по мере возникновения;
– временные — появляются нерегулярно и приводят к кратковременному снижению производительности системы связи или полному отказу сервисов. При высокой частоте возникновения они могут оказывать существенное влияние;
– короткие — приводят к малым потерям производительности или непродолжительным отказам сервисов, устраняются автоматически.

Симптомы отказов могут значительно отличаться друг от друга. Для обеспечения устойчивости узлов к сбоям применяется одна из двух методик: обмен информацией о проблемах между узлами сети или устранение отказов автоматически. В первом случае достоинством является то, что информация поступает в другие узлы сети. Это позволяет включить их в процесс устранения сбоев. Если же симптомы известны и отказ устранен в самом узле, то это делается автоматически.

Также важную роль играют последствия сбоев. Некоторые из них могут привести к немедленному отказу узла и, следовательно, к разрыву соединения, тогда как другие могут лишь обозначить «узкое» место системы.

Выбор алгоритмов восстановления нормального функционирования системы зависит и от источников проблемы. Система может реагировать по-разному на локальные сбои внутри узла и на проблемы, вызванные внешними причинами. Основная сложность в определении источника сбоя состоит в том, что часто одни сбои влекут за собой другие.

Степень поражения системы описывает важный аспект построения отказоустойчивых систем. Отдельные проблемы могут касаться только программных модулей, другие охватывают всю систему в целом. По степени воздействия возникающие отказы можно разделить на два класса.

1. «Жесткие» сбои. Этот вид характеризуется полным отказом системы. Например, разрыв соединения при отказе маршрутизатора.

2. «Мягкие» сбои. В этот класс входят сбои, которые вызывают негативные последствия, но не приводят к отказу всей системы. Например, высокий коэффициент ошибок на физическом уровне приводит к возникновению «узкого места». При появлении «мягких» сбоев применяется техника постепенного снижения показателей. Она заключается в контролируемом снижении функциональности или производительности системы. Это позволяет обеспечить определенный уровень работы системы вместо ее полного отказа [5].

Сбои могут быть упорядочены с помощью профилей ожидаемых сбоев, которые показывают, какие неисправности возможны в сети. Количественная оценка возможных сбоев и их последствий может отличаться в различных сетях.

Для адекватной реакции на сбои система должна их правильно идентифицировать. Процесс реакции системы на сбой включает в себя следующие аспекты:

– идентификация сбоев;
– снижение показателей;
– реакция на сбой;
– восстановление.

На сегодняшний день существуют различные подходы к классификации процесса идентификации сбоев: исключительно внутри компонента, непрерывно сравнивая с резервным работающим компонентом, контроль от узла к узлу и проверка с помощью диспетчера («ведущей станцией»). Эти подходы, в свою очередь, могут основываться на разных методиках. Контроль может быть пассивным и активным. При этом используются различные аудит-тесты, повторные вычисления, применяемые как самостоятельные тесты. Также возможны online-тесты, которые специально стимулируют сбой системы для контроля распознавания отказов.

Даже если проблема правильно идентифицирована, не всегда можно восстановить работоспособность системы в полном объеме. Особенно это часто встречается при «мягких сбоях» (например при высокой нагрузке), что ограничивает функциональность телекоммуникационной системы. С помощью методики снижения показателей можно обеспечить выполнение критических сервисов.

Реакция системы по устранению обнаруженной проблемы может быть очень различной. К online-мероприятиям, которые могут применяться в уже работающей системе, можно отнести сле-

дующие: возврат (откат) к контрольной точке, прогон, с одновременной коррекцией сбоев, повторное выполнение операций, которые были подвержены сбоям (или с теми же самыми или с другими ресурсами). Наряду с этим существуют меры, которые для проведения требуют только режима реального времени: реконфигурация архитектуры системы («на лету», с перезагрузкой), выполнение альтернативных задач (включая контролируемое завершение задач) и запрос ресурсов от внешних систем. Реакция системы на сбой может быть либо превентивной (например регулярные перезагрузки), проактивной (при появлении признаков сбоев) или реактивной (только при конкретных проявлениях сбоев).

После реакции системы на сбой необходимо восстановить ее нормальную работу.

Для этого могут потребоваться дополнительные ресурсы. Например, процедура восстановления может включать в себя инициализацию этих ресурсов.

Обнаружение и локализация сбоев являются одними из ключевых процессов восстановления системы. Среднее время на определение причин сбоя и его локализацию (mean- time-to-cause-and-location(MTTL)) [6] во многом определяет общее среднее время на восстановление системы.

Симптомы сбоев могут быть неоднозначными, непостоянными и неполными. Неоднозначность может возникать из-за похожести или идентичности симптомов для различных проблем. Непостоянство является следствием того, что для одних устройств какие-то компоненты работают неправильно, а для других эти же компоненты нормально функционируют. Из-за задержки или потери сообщений симптомы сбоев могут быть неполными. Задача системы локализации сбоев — справиться с этими факторами и принять непротиворечивое решение.

Возможна правильная интерпретация ненадежных данных для обнаружения сбоев с помощью систем, основанных на использовании предыдущих статистических сведений об ошибках в системе. Для точной локализации сбоя используются зависимости внутри сети, текущие конфигурации, информация о действующих сервисах и других неисправностях. Если симптомы кратковременны или система локализации сверхчувствительна, то могут возникать ложные срабатывания. Следовательно, система локализации сбоев в определенной степени ненадежна, что тоже следует учитывать.

Способность к определению причин сбоев. Зачастую, не только зависимые, но и независимые сбои могут возникать практически одновременно. Это ведет к совпадению сообщений о возникших неисправностях. Следовательно, нужно выделять причины сбоев и устранять их независимо.

В связи с этим предлагается описание цикла управления, определяющего необходимые концептуальные компоненты для обеспечения устойчивости телекоммуникационной системы.

Данная концепция устойчивости построена на основе работы J.P.G.Sterbenz др. [7], когда ряд принципов отказоустойчивости определяется стратегией сопротивляемости и называется D^2R^2 + DR: защита (defense), обнаружение (detection), исправление (rectification), восстановление(recovery), диагностика (diagnosis) и повышение качества (refinement). Стратегия описывает управление в реальном времени. Она позволяет проводить динамическую адаптацию сетей с учетом определенных задач, операции управления отображают прошлый оперативный опыт, а в режиме off-line цикл управления направлен на улучшение структуры сети.

Эта стратегия представляет собой системный подход к разработке отказоустойчивости сети. В ее основе лежит процесс управления, содержащий ряд концептуальных компонентов, которые реализуют в режиме реального времени аспект стратегии D^2R^2 +DR, и поэтому вводят в действие отказоустойчивость сети. Другие необходимые элементы, входящие в состав цикла управления устойчивости, являются производными, например устойчивость метрик, понимание проблем и рисков, распределение базы данных, основы политики управления.

На основе компонента стратегии в режиме реального времени D^2R^2 +DR был разработан процесс управления отказоустойчивостью, изображенный на рисунке, в котором контроллер вводит входные данные в систему под контроль, для того чтобы надлежащим образом управлять системой и ее выходными данными до желаемого эталонного значения.

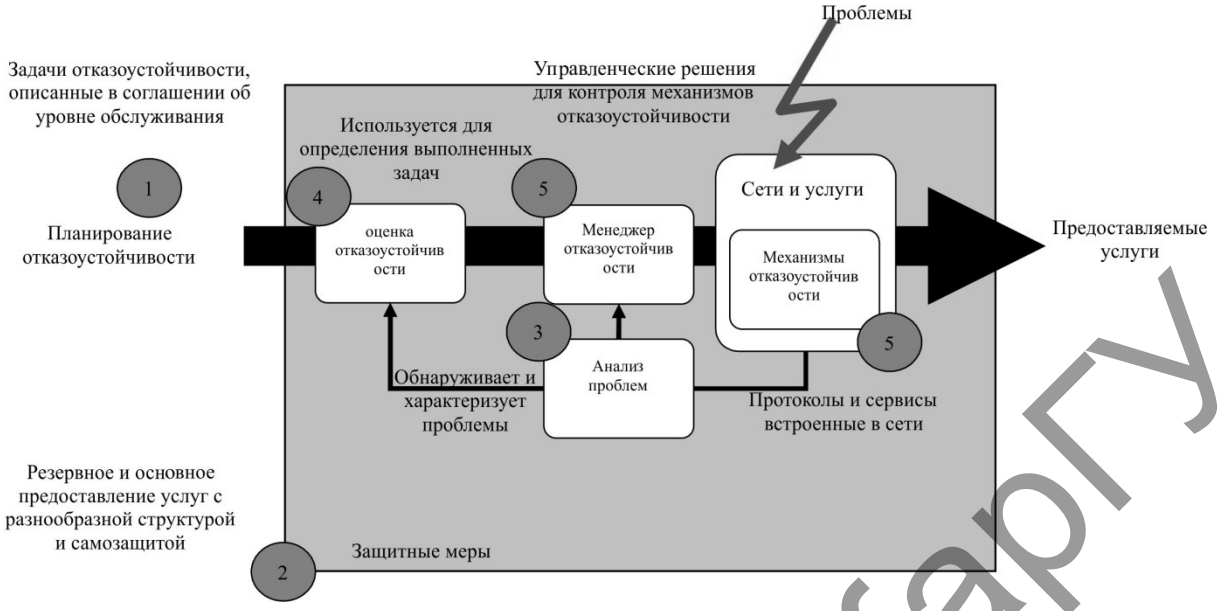

Рисунок. Процесс управления устойчивостью: происходит в режиме реального времени в компоненте стратегии устойчивости $D^2R^2 + DR$

Цикл управления формирует основу системного подхода к отказоустойчивости сети и определяет необходимые компоненты, которые являются производными. Их действия указаны на рисунке под соответствующими номерами.

1. Эталонное значение, которое стремятся достичь, выражается условием нормы устойчивости сети и описывается с помощью параметров устойчивости. Задачи отказоустойчивости отражают требования конечных пользователей, операторов сетей и поставщиков услуг.

2. Защитные меры должны быть приняты на месте активных действий для смягчения последствий проблем в сети и должны сохранить способность сети реализовать задачу устойчивости. Процесс определения задач, которые следует рассматривать в этой стратегии защиты (например, тех, которые происходят чаще и имеют поэтому большое влияние), является необходимым.

3. Несмотря на защитные меры, некоторые проблемы могут вызвать отклонение от норм устойчивости услуг, предоставляемых пользователям. Эти проблемы могут включать в себя непредвиденные атаки или неправильные конфигурации. Анализ компонентов позволяет обнаружить и охарактеризовать их, используя различные источники информации.

4. На основании анализа проблем делается вывод о состоянии сети, выполняется оценка устойчивости, определяется выполнение задачи отказоустойчивости сети в целом. Эта мера основана на отказоустойчивости показателей и зависит от механизмов эффективности защиты и восстановления при реагировании на вызовы.

5. Результаты выполнения анализа оценки устойчивости подаются менеджеру отказоустойчивости. И тогда ответственность за контроль устойчивости берут на себя механизмы, встроенные в инфраструктуру сети для обслуживания, чтобы сохранить предоставление необходимого уровня обслуживания и обеспечить постепенное уменьшение его возможностей при воздействии массовых угроз, а не обрыв связи. Эта адаптация направлена на использование сведений об отказоустойчивости, таких как политика и проблемы моделей сетей. Если проблема ослабевает, то расходы на восстановление неизбежной деградации качества обслуживания (QoS) уменьшаются. Следовательно, сеть должна восстанавливаться в нормальный режим работы после того, как проблема будет прекращена. Целью данного процесса в стратегии $D^2R^2 + DR$ является улучшение работы схемы управления устойчивостью, потому что она соответствует идеализированной работе системы. Такое улучшение могло быть реакцией на требование спроса, что приводит к новым нормам отказоустойчивости, новым проблемам и снижению эксплуатационных качеств. На стадии распознавания определены области для улучшения, в том числе защитные, которые вводятся в действие благодаря обработке.

Была разработана распределенная база данных проблем и их последствий (Distributed Store for Challenges and their Outcome — DISco), которая использует шаблон подписи сообщения для распространения информации между подсистемами в режиме реального времени. Такая информация пояс-

няет действия, выполняемые для обнаружения и устранения проблем. Источники информации могут сообщать больше данных, чем можно передать по сети, особенно в процессе вхождения. DlSco способен объединять информацию из различных источников для решения этой проблемы. Разрывание компонентов источников информации позволяет использовать обработку проблем анализа компонентов без необходимости изменять источники информации. Вспомогательные механизмы двух этапов цикла управления DlSco используют распределенную систему для долгосрочного хранения данных, которая знает о доступной емкости хранения и спроса.

Вывод. При управлении устранением последствий отказов решаются задачи контроля за состоянием сети и ее элементов в реальном масштабе времени; обнаружения и локализации неисправностей; восстановления связей; оперативного перестроения сети; устранения неисправностей; оповещение пользователей о проводимых работах.

Список литературы

1 *Дмитриев В.Н., Тушнов А.С., Сергеева Е.В*., Повышение эффективности системы мониторинга многозвенной сети передачи данных // Вестник АГТУ. — 2012. — №2.

2 *Małgorzata Steinder, Adarshpal S*. Sethi — A survey of fault localization techniques in computer networks — Science of Computer Programming 53, 2004. — P. 165–194.

3 *A.Avizienis, J.-C. Laprie and B*. Randell: Fundamental Concepts of Dependability. Research Report № 1145, LAAS-CNRS, April 2001.

4 *A.Bondavalli, L.* Simoncini — Failure Classification with respect to detection — IEEE CONFERENCE PUBLICATIONS. —1990. — P. 47–53.

5 *Paradis Lilia, Qi Han*, A Survey of Fault Management in Wireless Networks // Journal of Network and Systems Management. — № 9. — 2007.

6 Smith P. *et al.* Strategies for Network Resilience: Capitalizing on Policies. *AIMS 2010.* — Zurich. Switzerland. —2010. — June. — P. 118–22.

7 *J.P. G. Sterbenz et al.* Resilience and Survivability in Communication Networks: Strategies. Principles, and Survey of Disciplines. *Elsevier* Compute.' *Networks.* Special Issue on Resilient and Survivable Networks. — Vol. 54. — № 8. — 2010. — June. — P. 33–42.

С.В.Самоделкина, Г.Г.Таткеева, Г.Ш.Оразғалиев, В.И.Эйрих, А.Д.Мехтиев, В.В.Югай

Телекоммуникациялық жүйені басқару және ақпаратты беру үрдістеріне қабылдамаудың әсері

Мақалада қабылдамау әсерлерін жою және оларды локализациялауды басқару мәселелері қарастырылды. Жұмыс істеу беріктігіне, ақпаратты беру және тарату үрдісіне, байланыс жүйесін қайта іске асыру әдістеріне қабылдамау әсері сипатталды. Түйінділердің істен шығуының тұрақтылығын қамтамасыздандыру әдістері келтірілді. Проблемалар көздеріне байланысты жүйенің қалыпты қызмет ету алгоритмдері және істен шығу классификациясы ұсынылды. Жүйенің қызмет көрсетуінің тұрақтылығын қамтамасыз ету стратегиясы берілді.

S.V.Samodelkina, G.G.Tatkeyeva, G.Sh.Orazgaliyev, V.I.Eirikh, A.D.Mekhtiyev, V.V.Yugai

Influence of failure on telecommunication system and information transmission controlling processes

Questions of failures' consequences and their localization management are reviewed in this article. The influence of failures on the process of transmission and distribution of information and also on operational reliability and communication system's recovery methods are reviewed. Methods of nodes' failure sustainability are listed. A classification of faults is proposed, as well as recovery algorithms for normal functioning of the system, these algorithms depend on the source of the problem. Describe strategies to ensure sustainability of the network connection.

References

1 Dmitriyev V.N., Tushnov A.S. Sergeyeva Ye.V. *Improvement of monitoring system of multi-tier data transmission network. Messenger of AGTU*, № 2, 2012.

2 Małgorzata Steinder, Adarshpal S. *Sethi — A survey of fault localization techniques in computer networks* — Science of Computer Programming 53, 2004, p. 165–194.

3 Avizienis A., J.-C.Laprie and B. *Randell: Fundamental Concepts of Dependability*. Research Report № 1145, LAAS-CNRS, April 2001.

4 *A.Bondavalli, L. Simoncini — Failure Classification with respect to detection* — IEEE CONFERENCE PUBLICATIONS, 1990, p. 47–53.

5 Paradis Lilia, Qi Han, *A Survey of Fault Management in Wireless Networks, Journal of Network and Systems Management*, № 9, 2007.

6 Sterbenz J.P.G.*et al. Resilience and Survivability in Communication Networks: Strategies. Principles, and Survey of Disciplines*. *Elsevier* Compute.' *Networks.* Special Issue on Resilient and Survivable Networks, Vol. 54, № 8, June 2010, p. 33–42.

7 Smith P. *et al. Strategies for Network Resilience: Capitalizing on Policies. AIMS 2010.* Zurich, Switzerland, June 2010, p. 118–22.