Журнал «Вестник связи», №9, 2007

НАДЕЖНОСТЬ СЕТЕЙ СВЯЗИ В ПЕРИОД ПЕРЕХОДА К NGN

В.А. Нетес, начальник отдела НТЦ "КОМСЕТ", доктор технических наук

Автор этой статьи более 30 лет занимается вопросами надежности сетей и систем связи. С 1974 по 1993 гг. он работал в соответствующих подразделениях ЦНИИС. В середине 1990-х годов был членом Научно-методического совета Консультационного центра по качеству, надежности и безопасности при Государственном политехническом музее, выросшем из знаменитого Кабинета надежности, организованного еще в 1963 г. В настоящее время помимо работы в НТЦ "КОМСЕТ" преподает теорию надежности студентам МТУ СИ, является членом международного Гнеденко-Форума, объединяющего специалистов по надежности. Обе его диссертации: кандидатская (защищенная в ЦНИИС в 1982 г.) и докторская (защищенная в ИППИ РАН в 1995 г.), а также значительная часть публикаций (около 60) посвящены вопросам надежности.

Нужна ли России надежная связь?

Положительный ответ на этот вопрос кажется очевидным, и вряд ли кто-нибудь станет это оспаривать. Однако с тем, что обеспечение надежности требует принятия специальных и целенаправленных мер, проведения соответствующих исследований, испытаний, расчетов и т. п., согласны уже далеко не все. К сожалению, в последнее время мнение об отсутствии необходимости всего этого стало достаточно распространенным.

Такой взгляд нашел свое отражение даже в законотворчестве. Если в Федеральном законе "О связи" 1995 г. трижды указывалось на необходимость обеспечения надежности, то в действующем ныне законе 2003 г. таких упоминаний уже нет. Правда, в нем неоднократно говорится об обеспечении устойчивости функционирования единой сети электросвязи, но что понимается под этим понятием? Для прояснения ситуации стоит рассмотреть его эволюцию.

В течение многих лет под устойчивостью понималась совокупность трех свойств: надежности, живучести и помехоустойчивости [1]. Авторы монографии [1] указывали, что применение интегральной категории устойчивости не предполагает ликвидации составляющих ее понятий. При этом "надежность отражает влияние на работоспособность системы главным образом внутрисистемного фактора – случайных отказов техники... Живучесть же характеризует устойчивость системы связи против действия причин, лежащих вне системы и приводящих к разрушениям или значительным повреждениям некоторой части ее элементов". Подчеркивалось, что "надежность и живучесть – существенно различные понятия и самостоятельные проблемы, требующие своих решений при разработке и совершенствовании систем и сетей связи".

В 1994 г. появилась статья [2], авторами которой были руководители подразделений ЦНИИС, занимавшихся вопросами обеспечения устойчивости (кстати, отсутствие в настоящее время в ЦНИИС подобных подразделений – еще одно свидетельство снижения интереса к данной тематике). В ней давалось следующее определение: "Устойчивость – способность сети сохранять работоспособное состояние во времени и в условиях, создаваемых воздействиями внешних и внутренних ДФ" (ДФ – дестабилизирующий фактор). При этом пояснялось, что "устойчивость характеризуется свойствами надежности и живучести". Далее указывалось, что "свойство надежности должно обеспечивать функционирование сети связи и ее элементов в условиях действия внутренних непреднамеренных (случайных) ДФ", а "живучесть – свойство

сети сохранять способность выполнять требуемые функции в условиях, создаваемых воздействием внешних ДФ".

Наконец, в 2007 г. публикуется статья [3] (ее авторы – заместитель руководителя Федерального агентства связи РФ и генеральный директор Ассоциации сертификации "Связь"), в которой приводятся определения понятий устойчивости, целостности и безопасности единой сети связи, используемых в законах "О техническом регулировании" (2002 г.) и "О связи" (2003 г.). В частности, в ней дается следующее определение: "Устойчивость функционирования единой сети электросвязи – свойство сети связи выполнять свои функции при воздействии внешних дестабилизирующих факторов". Оно практически совпадает с приведенным выше определением живучести. Таким образом, в настоящее время устойчивость сети связи свелась фактически только к одному свойству живучести и перестала включать в себя надежность!

Пренебрежение вопросами надежности нередко обосновывается тем, что современные средства связи являются весьма надежными, а сети связи – разветвленными и допускающими обходы, поэтому отказы возникают очень редко, а если и возникают, то их последствия незначительны. С этим частично можно согласиться (только частично, ибо так обстоит дело далеко не везде и не всегда), однако каждый этап развития техники, давая ответы на одни вопросы, в то же время порождает новые. Это в полной мере относится и к обеспечению надежности сетей связи.

Почему сейчас вопросам надежности надо уделять серьезное внимание?

Во-первых, рост требований к качеству со стороны пользователей, обусловленный активным проникновением телекоммуникаций во все сферы жизни, и обострение конкуренции, вызванное либерализацией рынка, заставляют операторов все больше заботиться о качестве обслуживания (Quality of Service, QoS). Соглашения об уровне обслуживания (Service Level Agreement, SLA), заключаемые как с конечными пользователями, так и между операторами, становятся важным атрибутом взаимоотношений на современном рынке. А надежность является одним из важнейших факторов, влияющих на QoS, в силу чего требования к надежности (чаще всего к готовности) включаются практически во все SLA. При этом за "сверхнормативные" простои в SLA, как правило, предусматриваются штрафные санкции. Более подробно вопросы задания нормативов надежности и санкций за их нарушение в SLA рассмотрены в [4, 5].

Негативные последствия отказов не ограничиваются прямыми финансовыми потерями, обусловленными уменьшением доходов от предоставления услуг из-за простоев, и штрафными санкциями в случаях нарушения SLA. Нельзя забывать и о потерях, связанных с недовольством клиентов и ухудшением имиджа компании, которые обусловлены:

- оттоком недовольных клиентов к конкурентам;
- снижением привлекательности оператора в глазах потенциальных клиентов;
- снижением привлекательности компании в глазах существующих и потенциальных партнеров, акционеров и инвесторов.

Во-вторых, в настоящее время происходят радикальные перемены в технологиях связи. На смену коммутации каналов приходит коммутация пакетов, активно внедряются новые технологии транспорта и доступа, применяются новые протоколы. Такое обновление, тем более идущее быстрыми темпами, всегда чревато потерями, в том числе и в надежности. Это обусловлено тем, что, с одной стороны, на сетях связи

начинают использоваться недостаточно апробированные, сырые продукты и решения, а с другой, – эксплуатационный персонал компаний-операторов оказывается не подготовленным к их обслуживанию. В этой связи стоит еще раз обратить внимание на необходимость проведения тщательных и всесторонних испытаний нового оборудования, обучения специалистов его обслуживанию и вообще новым технологиям совершенствования эксплуатационных процессов.

Подобная ситуация уже имела место в прошлом. В конце 80-х – начале 90-х годов прошлого века в период активного внедрения ВОЛС, ОКС-7 и других новшеств на сетях связи США произошло несколько крупных аварий, вызвавших значительный общественный резонанс. Это заставило обратить на вопросы обеспечения надежности самое серьезное внимание. В частности, в 1991 г. был создан Совет по сетевой надежности (Network Reliability Council). Подробнее об этом можно прочитать в статье [6].

Помимо общих задач обеспечения надежности, обусловленных всяким техническим перевооружением, свои специфические проблемы выдвигает идущий в настоящее время активный переход к построению сетей связи в соответствии с принципами NGN. Более подробно они будут рассмотрены далее.

В-третьих, чтобы шагать в ногу со временем, оператору недостаточно закупить современное оборудование и ПО, начать предоставлять новые услуги. Нуждаются в обновлении и бизнес-процессы. Работы по реорганизации и совершенствованию бизнес-процессов ведутся сейчас в целом ряде операторских компаний. При этом, как уже отмечалось, важно не упускать из виду эксплуатационные процессы, в частности, обеспечения надежности. Этому вопросу также посвящен специальный раздел статьи.

Проблемы надежности NGN

Одной из проблемных областей при переходе к NGN является надежность. К сожалению, это обстоятельство понимается далеко не всеми руководителями и специалистами. Бытует мнение, что обеспечение надежности в NGN принципиально не отличается от решения этой задачи в традиционных сетях связи [7]. Более того, порой даже встречаются высказывания о бесспорном преимуществе NGN перед традиционными сетями с точки зрения надежности (например, в [8]). В действительности, ситуация с обеспечением надежности в условиях перехода к NGN является гораздо более сложной.

Помимо указанных выше общих задач обеспечения надежности, обусловленных всяким техническим перевооружением, свои специфические проблемы возникают в связи с некоторыми особенностями NGN, которые могут приводить к снижению надежности. При этом целесообразно выделить две составляющие: надежность коммутационного оборудования и надежность инфраструктуры IP. Более подробно они будут рассмотрены ниже.

В целом можно отметить, что инженерия надежности в NGN отличается от применяемой в сетях коммутации каналов [9], поэтому эта область требует проведения соответствующих исследований. В ряде развитых стран эти вопросы решаются на правительственном уровне. В частности, обеспечением надежности, устойчивости и безопасности будущих сетей серьезно обеспокоена Европейская комиссия. По ее заказу Alcatel-Lucent Bell Labs провела специальное исследование, по результатам которого

был подготовлен отчет, озаглавленный "Готовность и устойчивость инфраструктур электронных коммуникаций" [10].

Надежность коммутационного оборудования NGN

Для традиционных узлов с коммутацией каналов основной нормируемой составляющей надежности является готовность, требование к которой задавалось в виде "не более 2ч простоя за 20 лет службы", что соответствует значению коэффициента готовности "пять девяток", т.е. 0,99999 [8].

При переходе к NGN место традиционного узла коммутации занимает гибкий коммутатор (Softswitch). Возникает комплекс из большого числа отдельных устройств (контроллеров, шлюзов, серверов). Все они имеют высокую надежность: значение коэффициента готовности каждого из них, как обычно заявляют производители, составляет все те же "пять девяток". Однако для выполнения функций узла коммутации необходима совместная работа нескольких таких устройств, поэтому результирующая надежность будет равняться произведению их коэффициентов готовности, т.е. в итоге оказывается более низкой.

Еще более важным фактором, негативно влияющим на надежность NGN, является централизация управления процессами обслуживания вызовов. Ключевым элементом структуры становится контроллер шлюзов или сервер вызовов (Softswitch в узком понимании этого термина). При этом один такой котроллер или сервер управляет многими шлюзами, поэтому его отказ может привести к прекращению работы сети на большой территории. Подобная ситуация негативно влияет не только на надежность, но и на живучесть сети. На это обстоятельство и связанные с этим риски уже обращали внимание в своих публикациях руководители Управления связи Федерального агентства связи [11, 12].

Неслучайно ведущие производители оборудования NGN предусматривают возможность резервирования контроллеров шлюзов, в том числе с географическим разнесением. Некоторые операторы связи учитывают необходимость подобного резервирования при проектировании своих сетей [13,14]. К сожалению, часто из соображений экономии это не делается. Это противоречит одному из основных принципов построения отказоустойчивых систем, каковыми и должны быть современные сети связи, – отсутствию в структуре "единой точки отказа".

Все указанные обстоятельства требуют изучения, для компенсации указанных негативных факторов должны разрабатываться и применяться соответствующие схемы и методы резервирования. При этом они должны реализовываться как на аппаратурном, так и на сетевом уровне.

Надежность сетей IP

Характерной тенденцией NGN является широкомасштабное использование сетей на основе протокола IP. Методы оценки и обеспечения надежности таких сетей разработаны пока недостаточно. Работа в этом направлении ведется в ряде зарубежных стран. В частности, в Финляндии разрабатывается исследовательский проект IPLU (это сокращение от его полного названия "Методы оценки надежности сетей IP" на финском языке) [15]. В рамках этого проекта в мае 2006 г. был проведен международный семинар, который отметил актуальность этой тематики, подвел итоги проведенных исследований, наметил направления дальнейшей работы.

Достоинством сетей IP является возможность предоставлять множество альтернативных путей передачи информации. Именно по этой причине в [8] и делается вывод о преимуществе решений NGN с точки зрения надежности. Распространено даже мнение, что разработчики Интернета и лежащих в его основе протоколов ставили своей целью создание сети, способной обеспечить связь в условиях выхода из строя некоторых сетевых элементов, в том числе в условиях военных действий. Однако в действительности это не более чем миф [16].

Однако для реализации указанного преимущества необходимо иметь достаточно разветвленную физическую инфраструктуру. Только в этом случае различные маршруты будут разделены не только логически, но и физически. Иначе они могут проходить, например, в общем кабеле, обрыв которого приведет к неработоспособности всех проходящих по нему путей. Такая ситуация нередко встречается на практике.

Кроме того, время перехода на новые пути передачи информации в сетях IP слишком велико для трафика реального времени, и если не принять дополнительных мер защиты, такое переключение приведет к разрывам соединений. Поэтому механизмы быстрого восстановления часто реализуются на физическом уровне. А здесь наблюдается переход от технологии SDH, имеющей различные стандартизованные механизмы резервирования, обеспечивающие высокую отказоустойчивость сети, к более дешевой, но не имеющей пока подобных механизмов технологии Ethernet. Это также негативно влияет на надежность сети [15].

Наконец, указанное выше достоинство имеет и оборотную сторону. Существенной особенностью сетей IP с точки зрения надежности является то, что в них появляется новый источник отказов – сбои в работе протоколов маршрутизации. Эти протоколы (в частности, BOP) имеют проблемы со стабильностью и весьма чувствительны к ошибкам конфигурации [15]. При этом в силу особенностей работы протоколов маршрутизации подобные нарушения могут распространяться по сети лавинообразно. На это обстоятельство также обращает внимание в своем отчете Проблемная группа по NGN Консультативного комитета по связи для национальной безопасности при Президенте США [17]. Вообще, стоит отметить, что приложение G к этому отчету содержит детальный анализ всех угроз и уязвимостей NGN.

Рекомендация МСЭ-Т G.1000 [18] указывает, что использование сетей и служб на основе IP выдвигает целый ряд проблем, таких как отсутствие апробированных, надежных и масштабируемых механизмов для решения целого ряда задач, в частности, быстрого и полного восстановления связности на уровне IP после серьезных простоев (или атак) в сильно загруженных сетях.

Реальным и конкретным примером, показывающим опасность перехода к инфраструктуре на основе IP, является выход из строя значительной части сети IP японского оператора NTT, имевший место 15 мая 2007 г. [19]. При этом от 2 до 4 тыс. маршрутизаторов производства Cisco прекратили работу, и их неработоспособность продолжалась около 7 ч. В результате миллионы пользователей в большей части Восточной Японии потеряли связь. Первопричиной события стало переключение на резервные маршруты, вызвавшее некорректное обновление маршрутных таблиц, что и привело к массовой неработоспособности маршрутизаторов.

Для уменьшения опасности возникновения подобных ситуаций необходимо:

- тщательное тестирование нового оборудования и ПО, в том числе при стрессовых нагрузках, с имитацией ошибок и отказов отдельных технических средств и т.п.;
- применение средств сетевого мониторинга, позволяющих быстро выявлять и локализовывать неисправности;
- наличие эксплуатационного персонала, численность и квалификация которого позволяли бы вести мониторинг сети и оперативно устранять возникающие неисправности;
- обеспечение технической поддержки со стороны производителей сетевого оборудования.

Процессы эксплуатации и совершенствования бизнес-процессов

Как показывают результаты проведенного в ЦНИИС анализа [20], "осложнения в организации эксплуатации сетей связи следующего поколения обусловлены в первую очередь изменением конфигурации сети и зон ответственности персонала. Сегодня неисправности на сети устраняются локально, на месте, а в распределенной сети следующего поколения это должно делаться централизовано. Пока у руководящего персонала оператора связи недостаточно опыта по организации, контролю и управлению эксплуатацией сетей NGN, а у технического персонала – опыта обслуживания нового оборудования". Ряд проблем, связанных с управлением и эксплуатацией NGN, отмечен также в [21].

В этой связи чрезвычайно полезными для операторов связи будут разработки международного Форума управления телекоммуникациями (TM Forum, TM Форум), направленные на совершенствование бизнес-процессов, построение современных OSS и т. п. В частности, одной из важнейших разработок TM Форума является эталонная модель процессов оператора связи eTOM (enhanced Telecom Operations Map – расширенная карта процессов телекоммуникационной компании). Она принята МСЭ-Т (группа рекомендаций M.3050) и использована при выработке принципов организации управления NGN (Рекомендация M.3060/Y.2401).

Хочется подчеркнуть, что eTOM представляет собой не какие-то абстрактные умозрительные построения, а активно используется ведущими мировыми операторами связи и производителями и является обобщением их опыта.

К сожалению, в нашей стране применение eTOM нередко ограничивается финансово-экономической сферой и взаимоотношениями с клиентами, поставщиками и партнерами, а внутренние эксплуатационные процессы, в том числе те, которые направлены на обеспечение надежности, зачастую остаются за рамками рассмотрения. Это можно объяснить несколькими причинами.

Во-первых, само слово "бизнес" в русском языке имеет более узкий смысл, чем в английском, который является рабочим языком TM Форума и на котором написаны его документы. Первое значение английского слова business – дело, занятие (Англо-русский словарь В.К. Мюллера). Поэтому под бизнес-процессами в документах TM Форума понимаются вообще все процессы, относящиеся к деятельности компании. В русском языке "бизнес – предпринимательская экономическая деятельность, приносящая доход, прибыль" (Толковый словарь русского языка С.И. Ожегова и Н.Ю. Шведовой). Соответственно этому более узко воспринимается и словосочетание "бизнес-процесс".

Во-вторых, многие консультанты, оказывающие операторам связи услуги по описанию и совершенствованию бизнес-процессов на основе eTOM, не являются специалистами в области телекоммуникаций и слабо представляют принципы функционирования и эксплуатации сетей связи. Поэтому они не могут полноценно заниматься эксплуатационными процессами.

В-третьих, высшее руководство компаний, в первую очередь, озабочено финансовыми показателями, поэтому приоритет отдается процессам, непосредственно связанным с денежными потоками.

Разумеется, такой подход нельзя считать правильным. Пренебрежение эксплуатационными процессами приводит к снижению качества обслуживания, авариям на сетях, необходимости преждевременного обновления или замены оборудования и, как следствие, к финансовым потерям.

В области операционных процессов eTOM имеется целый ряд процессов, направленных на обеспечение надежности. При этом речь идет не только об обнаружении и устранении возникающих отказов, за что отвечает процесс "Управление проблемами с ресурсами" (это процесс 2-го уровня декомпозиции, входящий в вертикальную группу процессов "Обеспечение"), но и о предупреждении их возникновения. Этой цели служит процесс "Поддержка управления проблемами с ресурсами" (3-й уровень, вертикальная группа "Поддержка и готовность операционных процессов"). Он осуществляет проактивное управление выполняемыми на основании статистических данных действиями по профилактическому и плановому техническому обслуживанию и ремонту инфраструктуры ресурсов, а также охватывает мониторинг, управление и отчетность для процессов управления проблемами с ресурсами.

Краткие выводы

Итак, задачи обеспечения надежности нисколько не потеряли своей актуальности в современных телекоммуникациях. Напротив, целый ряд тенденций – рост требований к QoS и применение SLA, переход к NGN, совершенствование бизнес-процессов – настойчиво требуют уделять им самое серьезное внимание. Отказы в сетях связи влекут финансовые и прочие потери для операторов. Нельзя упускать из виду, что ряд характерных особенностей NGN могут приводить к снижению надежности. Поэтому вопросы ее обеспечения должны быть в сфере внимания руководителей и специалистов регулирующих и контролирующих органов, операторов связи, производителей оборудования, системных интеграторов, проектных, исследовательских и образовательных организаций.

Литература

1. Надежность и живучесть систем связи / Под ред. Дудника Б.Я. // М.: Радио и связь, 1984.
2. Киселев Л.К., Маркелов А.П., Воробьев Б.В. Концептуальные основы обеспечения устойчивости сетей связи // Электросвязь. 1994. № 2.
3. ЮрасоваЛ.В., Кондратов С.Ф. Проблемы разработки нормативных правовых актов по вопросам применения средств связи // Электросвязь. 2007. № 3.
4. Нетес В.А. Соглашения об уровне обслуживания: стандарты и реалии // Вестник связи. 2003. № 8.
5. Нетес В.А. Задание требований по надежности в соглашениях об уровне обслуживания // Электросвязь. 2004. № 4.

6. Нетес В.А. Надежность сетей связи: тенденции последнего десятилетия // Электросвязь. 1998. № 1.
7. Витченко А., Соколов Н., Стрижков В. Построение сети NGN в Ленинградской области // Connect! Мир связи. 2007. № 4.
8. Гольдштейн Б.С. 10 лет эволюции коммутационной техники // Вестник связи. 2007. № 5.
9. Tortorella M. Reliability engineering challenges of converged networks and packet-based services: Rutgers' Industrial Engineering Working Paper. February 5, 2003.
10. Availability and Robustness of Electronic Communications Infrastructures. "The ARECI Study": Final Report // European Commission. March 2007.
11. Леваков А.К. Особенности создания и функционирования сетей связи нового поколения//Фотон-Экспресс. 2006. № 5.
12. Букринский С.А. Проблема обеспечения устойчивости, живучести и безопасности сетей связи - основная задача управления сетями следующего поколения//4-я Междун. конф. "Управление сетями электросвязи - основа надежности функционирования телекоммуникационной инфраструктуры". М., 2006.
13. Панин И.Е. Нужны ли технологии NGN сегодня?//Фотон-Экспресс. 2005. №7.
14. Леваков А.К. Некоторые структурно-сетевые решения построения сетей местной и зоновой телефонной связи с технологией NGN в Московской области // 6-я Ежегодная междун. конф. "NGN в России. Технологии и услуги". СПб, 2007.
15. Norros I. A broad approach to the dependability of IP networks // European CUP Newsletter. 2006. Vol. 2. No 3.
16. Нетес В.А. Уроки Интернета // Вестник связи. 2006. № 4.
17. Next Generation Networks Task Force Report // The President's National Security Telecommunications Advisory Committee. March 28, 2006.
18. ITU-T Recommendation G.1000 (11/2001). Communications Quality of Service: A framework and definitions.
19. Duffy J. Cisco routers caused major outage in Japan: report// Network World. 16.05.2007.
20. NGN-проблемы // Вестник связи. 2006. №12.
21. Нетес В.А. Проблемы управления сетями связи следующего поколения // 4-я Междун. конф. "Управление сетями электросвязи - основа надежности функционирования телекоммуникационной инфраструктуры". М., 2006.