Анализ живучести мультисервисных сетей связи, построенных по технологии PON

Ключевые слова: *пассивные оптические сети (PON), вредные воздействия, живучесть, избыточность, устойчивость.*

Анализируются принципы построения пассивных оптических сетей, приводится характеристика вредных воздействий, которым они подвержены, дается оценка живучести сетей PON и рассматриваются методы ее повышения.

Саморуков А. П.,
магистрант МТУСИ,
strapel@mail.ru

1. Введение. Проблема повышения живучести сетей доступа, построенных на основе технологии PON (аббр. от англ. Passive optical network), в последние годы приобретает все большее и большее значение. Проектирование новых мультисервисных сетей связи, использование и развитие уже существующих напрямую связаны с проблемами обеспечения и повышения их живучести.

Технология пассивных оптических сетей PON – относительно молодая, постоянно развивающаяся технология, и на сегодняшний день имеется лишь малая часть работ, в той или иной степени затрагивающих вопросы, связанные с исследованием живучести сетей связи, построенных на основе данной технологии. В связи с этим, исследование живучести пассивных оптических сетей доступа и разработка методов повышения их живучести, является достаточно актуальной темой.

Живучесть наряду с понятием надежности относится к числу важнейших характеристик сетей доступа, а также сетей телекоммуникаций в целом. Под живучестью понимается свойство сети сохранять свою работоспособность под воздействием вредных факторов, способных вызвать повреждения отдельных её участков. Живучесть – это показатель устойчивости, характеризующий эффективность работы системы в условиях нарушения работы ее отдельных элементов [1]. Важность обеспечения работоспособности мультисервисных сетей связи, построенных на основе технологии PON, является необходимым условием для их нормального функционирования и дальнейшего развития.

2. Технология PON. В настоящее время технология PON считается одной из наиболее перспективной технологии широкополосного доступа по оптоволоконному каналу. Это быстро развивающаяся, одна из наиболее эффектных технологий для построения сетей мультисервисного доступа на участке «последней мили». Такие сети благодаря своей долговечности, малому затуханию оптического сигнала и огромной пропускной способности позволяют в полной мере раскрыть экономический потенциал семейства архитектур FTTx (англ. fiber to the x – оптическое волокно до точки X).

На основе технологии PON строятся полностью пассивные оптические сети связи древовидной топологии с центральным узлом OLT (optical line terminal) и абонентскими узлами ONU (optical network unit). Центральный узел OLT обеспечивает соединение с магистральным участком сети и абонентскими узлами ONU, осуществляя прием и передачу данных. На участках ветвления дерева устанавливаются пассивные компоненты – сплиттеры (разветвители), полностью независимые от питания и обслуживания. Центральный узел OLT может содержать несколько приемопередающих модулей, обеспечивающих передачу информации абонентским узлам ONU, каждый из которых может обеспечивать высокоскоростной доступ в Интернет сотням абонентов.

Технология PON включает в себя два главных стандарта: IEEE 802.3ah Ethernet PON (EPON) и ITU-T G.984 Gigabit PON (GPON). Оба стандарта предусматривают передачу прямого (нисходящего) потока на длине волны 1490 нм и обратного (восходящего) потока на длине волны 1310 нм, при этом передача осуществляется по принципу временного мультиплексирования (англ. Time Division Multiplexing, TDM). Каждому абонентскому узлу ONU отводится отрезок времени (time slot) для передачи данных с учетом задержки сигналов, в результате чего исключается пересечение сигналов поступающих от разных абонентских устройств ONU. После объединения общий восходящий поток содержит сигналы от всех пользователей.

3. Характеристика вредных воздействий на мультисервисные сети связи. Вредное или негативное воздействие – это воздействие (событие, процесс, явление), способное нанести потенциальный вред сетевым ресурсам. Вредным воздействием на мальтисервисную сеть связи будем называть любое воздействие на ее компоненты, способное вызвать повреждение или уничтожение активных (оконечные оптические блоки) и пассивных составляющих сети, а также привести к потере, искажению и блокированию доступа к информации, передаваемой по сети связи.

Классификация вредных воздействий на сети связи может быть проведена по ряду базовых признаков. Выделяют семь наиболее важных групп таких признаков [2]:

– по природе возникновения.

– по степени преднамеренности проявления.

– по непосредственному источнику вредных воздействий.

– по положению источника вредных воздействий.

– по этапам доступа пользователей или программ к ресурсам сетей связи.

– по способу доступа к ресурсам сетей связи.

– по степени воздействия на сети связи.

Для мультисервисных сетей связи негативные воздействия можно представить в виде множества $L = \{L_1, L_2, L_3, L_4, L_5\}$ в соответствии с сетевой моделью OSI (англ. open systems interconnection basic reference model – базовая эталонная модель взаимодействия открытых систем).

Первая группа $\{L_1\}$ представляет собой негативные воздействия на физическом уровне. Такие воздействия могут быть как природного происхождения, так и искусственного (диверсионные и террористические акты) и направлены на функциональные элементы сети связи, работающие со средой передачи, сигналами и двоичными данными. В мультисервисных сетях воздействия данной группы приводят к уничтожению или повреждению каналов связи, а также коммутационного оборудования, что приводит к нарушению обмена информацией между абонентами. Также в данную группу можно включить несанкционированные подключения к коммутационным портам и оптоволоконным каналам связи.

Вторая группа $\{L_2\}$ – комплекс воздействий на канальном уровне. На данном уровне различного рода трафик (IP, речь, видео) инкапсулируется в кадры и осуществляется физическая адресация. Здесь возможен несанкционированный доступ к ресурсам сети со стороны злоумышленников приводящий к блокированию или уничтожению соединения. В сетях PON для защиты от несанкционированного доступа используется шифрование сетевого трафика, что позволяет существенно повысить безопасность передачи, как служебной информации, так и личной информации абонентов.

Третья группа $\{L_3\}$ – совокупность воздействий на сетевом уровне, отвечающего за определение маршрута и логическую адресацию. В данную группу входят замена адресной информации в служебных блоках, подмена записей в базах локального интерфейса управления, подмена записей в базах межсетевого интерфейса. Все это может привести к уничтожению одного или нескольких соединений и потере информации.

Третья группа $\{L_4\}$ — воздействия на транспортном уровне, отвечающем за прямую связь между конечными пунктами (отправителями и адресатами) и надежность. Данный уровень включает в себя следующие негативные воздействия: нарушение и уничтожение соединения, изменение типа передаваемых данных, параметров обслуживания, связей между функциональными элементами и т.д. Для защиты соединения на транспортном уровне (TCP-соединения) применяется система шифрования данных на стороне отправителя и дешифровка на стороне адресата.

Пятая группа $\{L_5\}$ – воздействия на верхнем уровне модели OSI, обеспечивающем взаимодействие пользовательских приложений с сетью. Сюда входят несанкционированный доступ и съем информации с каналов связи и узлов коммутации, приводящие к потере пользовательской информации и установленного соединения.

4. Классификация угроз в сетях PON. Все сети, использующие множественный доступ, в том числе и сети PON, обладают серьезным недостатком. Этот недостаток связан с наличием общего канала передачи данных, в результате чего возможен выход из строя целого сегмента сети PON из-за действий злоумышленника или неисправностей сетевого оборудования. Помимо этого в сетях PON затруднена диагностика состояния сети, особенно в случае отсутствия контрольных точек, а также усложнена задача поиска злоумышленников.

Самым уязвимым местом в пассивных оптических сетях является физическая среда передачи данных, помимо нее атакам подвержены коммутаторы (оптические линейные терминалы), разветвители и WDM-мультиплексоры.

Источники угроз в сетях PON (рис. 1):

1) Снятие информации с волоконно-оптической линии. В местах изгиба и в местах сварных соединений оптического кабеля световые лучи могут выходить за его пределы. При повреждении изоляции оптического кабеля и подключении специальных средств для регистрации излучения с поверхности волокна, злоумышленник получает доступ к данным, передающимся через оптический кабель. Зафиксировать утечку информации на концах кабеля практически невозможно.

2) Атака на оптические разветвители и WDM-мультиплексоры. WDM-мультиплексоры (Wavelength Division Multiplexing – спектральное уплотнение каналов) применяются для увеличения пропускной способности абонентских каналов связи, путем передачи на разных несущих частотах нескольких информационных потоков по одному оптическому волокну. Оптические разветвители и мультиплексоры могут быть установлены в общедоступных местах. Для их защиты применяются оптические распределительные шкафы (ОРШ), выполненные в антивандальном исполнении и имеющие комбинированные замки.

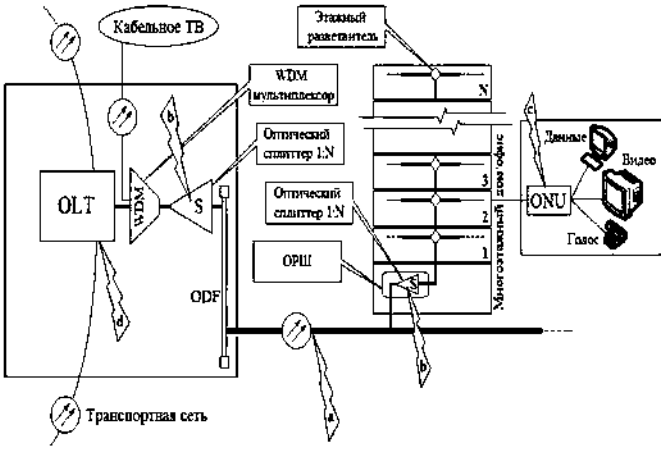

Рис. 1. Источники угроз в сетях PON:
a – снятие информации с волоконно-оптической линии;
b – атака на оптические разветвители и WDM-мультиплексоры;
c – перепрограммирование оконечного оборудования;
d – атака на стыке сетей.

3) Перепрограммирование оконечного оборудования. Основной особенностью всех PON сетей является то, что нисходящий поток достигает все оптические сетевые блоки (ONU), подключенные к сети. Злоумышленник после некоторых манипуляций с перепрограммированием ONU может добиться того, что будет получать информацию, адресованную другим пользователям. Система безопасности PON сетей должна уметь противостоять такого рода угрозам [3].

4) Атака на стыке сетей. Центральный сервисный модуль линейного терминала OLT находится на стыке между локальной и глобальной сетями. Он содержит коммутатор/маршрутизатор 2, 3 уровня и системный контроллер, позволяющий оператору подключиться к системе управления: локально – через порт RS-232 (RJ-45) или дистанционно – через внешнюю сеть. В данном случае

атакующим может быть нарушена конфиденциальность, целостность и доступность информации при ее обмене между внешней транспортной сетью и сетью PON.

Угрозы сети PON в оконечном оборудовании:

– ошибочные действия администратора сети и обслуживающего персонала, приводящие к потере или компрометации информации, а также ошибки пользователей;

– внесения изменений в программное обеспечение оконечного оборудования обслуживающим персоналом;

– несанкционированное копирование информации с носителей оконечного оборудования обслуживающим персоналом или пользователями.

Угрозы информации в линиях связи:

– прослушивание каналов связи;

– повреждение кабельной линий связи;

– уничтожение или искажение информации проходящей по линиям связи;

– внедрение ложных сообщений в общий поток, а также сетевых вирусов.

5. Анализ живучести сетей PON по показателю СДП. Средняя длина пути (СДП) является важнейшим эксплуатационным показателем сетей связи. Чем меньше СДП, тем меньше ее уязвимость, тем больше ее живучесть при разрыве одной дуги. Установлено [4], что средняя относительная длина пути (СОДП) по линейной и звездообразной сетям является прямым отражением их уязвимости при разрыве одной дуги. Необходимо проанализировать основные топологии построения сетей PON по характеру изменения СОДП в зависимости от размера сети.

Рассмотрим три топологии построения сетей PON. Будем считать оптические разветвители транзитными узлами, осуществляющими разделение потока оптического излучения между абонентскими узлами. В сети PON передача информации между узлами OLT и ONU осуществляется как в прямом, так и в обратном направлении, поэтому сеть будем считать полнодоступной с учетом того, что оптические разветвители осуществляют лишь транзит информации.

Топология «Звезда», представленная на рис. 2, применяется при плотном расположении абонентских узлов в районе АТС. Данная топология характеризуется минимальным количеством оптических разветвителей и единственным местом их установки.

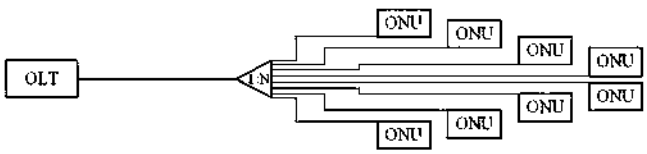

Рис. 2. Топология «Звезда»

В звездообразной сети PON сумма длин путей от центрального узла OLT до периферийных узлов ONU равна

$$L_c = l(n-1), \quad (1)$$

где l – средняя длина дуги; n – число оконечных узлов (размер сети).

Общее число соединений в сети PON при НУЭ (нормальные условия эксплуатации):

$$\gamma = 2(n-2). \quad (2)$$

Общая сумма длин между всеми парами узлов сети PON равна

$$\sum_{i=1}^{n}\sum_{j}^{n-1} D_{ij} = 4l(n-2). \quad (3)$$

СДП в звездообразной сети PON:

$$D_{ij} = 2l, \ (l = const). \quad (4)$$

С увеличением размера звездообразной сети PON СДП остается постоянной, равной $2l$. Уязвимость сети или СОДП при этом:

$$D(\beta) = \frac{D_{ij}}{L_c} = \frac{2}{n-1}. \quad (5)$$

Живучесть при этом

$$D(\alpha) = 1 - D(\beta) = \frac{n-3}{n-1}. \quad (6)$$

С увеличением размера уязвимость звездообразной сети PON при разрыве одной дуги уменьшается, стремясь к 0, живучесть возрастает, стремясь к 1. На рис. 3. показана зависимость живучести звездообразной сети PON от ее размера при разрыве одной дуги в сравнении с другими сетями (линия, звезда). Из рисунка видно, что сеть PON уступает по живучести классической «звезде», но с увеличением n стремится вместе с ней к 1, а также значительно превосходит по живучести линейную сеть при n > 5.

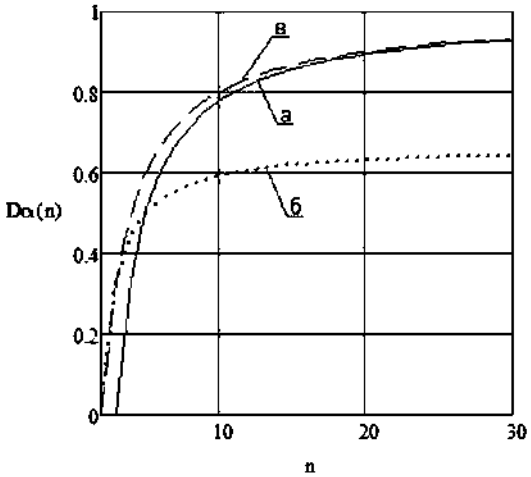

Рис. 3. Зависимости живучести сетей от их размера при разрыве одной дуги: *а* – звезда PON; *б* –линейная сеть; *в* – звездообразная сеть

Топология «шина» представлена на рис. 4. Данная топология применяется при расположении абонентских узлов вдоль оптической магистрали.

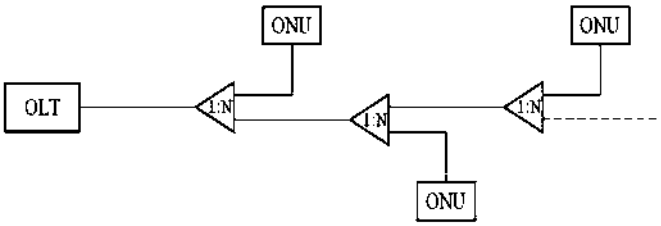

Рис. 4. Топология «Шина»

Топология «Шина» предполагает учет количества абонентских каскадов k для расчета общего числа соединений в сети PON при НУЭ, так как в каждом каскаде может быть от одного до нескольких оконечных сетевых устройств ONU:

$$\gamma = 2\left[n - (k+1)\right]. \quad (7)$$

Сумма длин путей от OLT до ONU определяется также как для топологии «Звезда». Общая сумма длин между всеми парами узлов сети PON равна

$$\sum_{i=1}^{n}\sum_{j}^{n-1} D_{ij} = \frac{l(n^2+6n-8)}{4}, \quad (8)$$

с учетом того, что $k = n/2 - 1$, т.е. по одному узлу на каскад (рис. 4). В этом случае наращивание узлов осуществляется бинарным образом (оптический разветвитель плюс абонентский узел ONU).

СДП в сети PON с шинной топологией:

$$D_{ij} = \frac{l(n^2+6n-8)}{4n}, \ (l = const). \quad (9)$$

Уязвимость сети или СОДП при этом:

$$D(\beta) = \frac{D_{ij}}{L_c} = \frac{(n^2+6n-8)}{4n(n-1)}. \quad (10)$$

С увеличением размера сети PON живучесть при разрыве одной дуги возрастает, стремясь к ¾, т.е.

$$\lim_{n\to\infty} D(\alpha) = \frac{3}{4}. \quad (11)$$

На рис. 5 показана зависимость живучести сети PON с шинной топологией от ее размера при разрыве одной дуги в сравнении с другими сетями (линия, звезда PON). Шинная топология уступает звездообразной и линейной по живучести, однако, после n>12 превосходит линейную в пределе на 1/12.

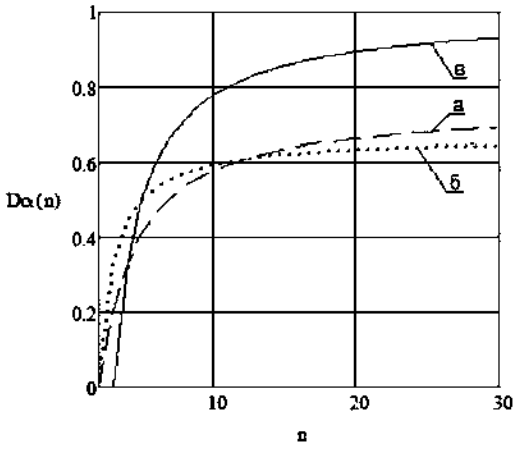

Рис. 5. Зависимости живучести сетей от их размера при разрыве одной дуги: *а* – шина PON; *б* – линейная сеть; *в* – звездообразная сеть PON

Древовидная топология применяется при разнесенном расположении абонентов (рис. 6). Оптимальная выходная мощность разветвителей между различными ветвями дерева рассчитывается путем подбора коэффициентов деления оптических разветвителей. Данная топология характеризуется гибкостью с точки зрения потенциального развития и удобством расширения абонентской базы.

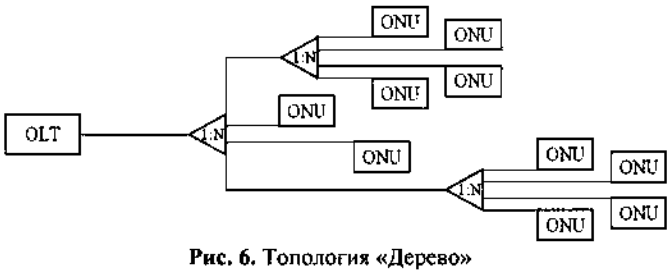

Рис. 6. Топология «Дерево»

В сети PON древовидной топологии размер сети определяется как

$$n = ab + a + 2, \quad (12)$$

где a – число дуг, исходящих из разветвителя фидерного волокна (волокна между узлом OLT и ближайшим разветвителем); b – число дуг, исходящих из периферийных разветвителей.

Сумма длин путей от центрального узла OLT до периферийных узлов ONU при этом равна

$$L_c = l(ab + a + 1). \quad (13)$$

Общее число соединений в сети PON при НУЭ:

$$\gamma = 2ab. \quad (14)$$

Общая сумма длин между всеми парами узлов сети PON:

$$\sum_{i=1}^{n}\sum_{j}^{n-1} D_{ij} = 6l \cdot ab. \quad (15)$$

СДП в сети PON древовидной топологии:

$$D_{ij} = 3l, \ (l = const). \quad (16)$$

С увеличением размера сети PON топологии «дерево» СДП остается постоянной, равной $3l$. Уязвимость сети или СОДП при этом:

$$D(\beta) = \frac{D_{ij}}{L_c} = \frac{3}{n-1}. \quad (17)$$

Живучесть сети:

$$D(\alpha) = \frac{n-4}{n-1}. \quad (18)$$

С увеличением размера живучесть сети PON древовидной топологии при разрыве одной дуги возрастает, стремясь к 1. На рис. 7. показаны зависимости живучести сетей PON рассмотренных топологий («звезда», «шина», «дерево»).

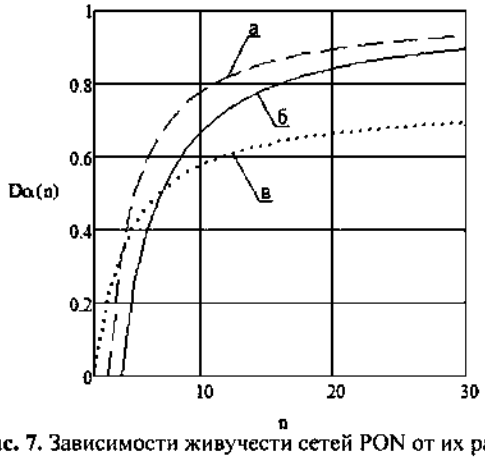

Рис. 7. Зависимости живучести сетей PON от их размера при разрыве одной дуги: а – «Звезда»; б – «Дерево»; в – «Шина»

Из проведенного анализа живучести сетей PON по показателю СДП можно сделать вывод, что наибольшей живучестью обладает звездообразная сеть PON, наименьшей – сеть PON с топологией шина. Для всех рассмотренных сетей средняя относительная длина пути является показателем их уязвимости, как было отмечено в [2] для линейных и звездообразных сетей. В сетях PON все соединения проходят через центральный узел OLT, в результате работоспособность сетей напрямую зависит от вероятности поражения центра или дуги, соединяющей OLT с оптическим разветвителем фидерного волокна.

6. Резервирование сетей PON. Повышение уровня защищенности является важной составляющей в обеспечении живучести и устойчивого режима функционирования сетей PON. Применяются четыре различные схемы защиты сетей PON [3], основанные на резервировании, т.е. введении в сеть связи структурной избыточности с целью повышения степени связности отдельных ее элементов, это:

Фидерное резервирование. Данная схема защиты обеспечивает частичное резервирование только фидерного волокна. Схема фидерного резервирования представлена на рис. 8, где LT – приемопередающий модуль, S – оптический разветвитель. При повреждении фидерного волокна происходит потеря связи с целым сегментом сети, поэтому данный участок является наиболее приоритетным для резервирования.

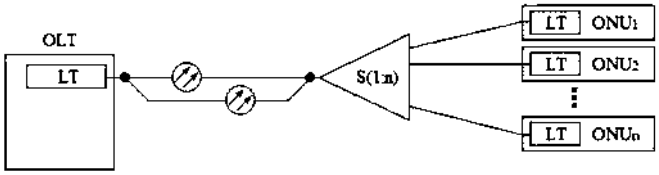

Рис. 8. Схема фидерного резервирования

Частичное резервирование со стороны OLT. В данном случае дополнительно резервируется OLT и участок фидерного волокна. Центральный узел OLT оборудуется двумя приемопередающими модулями (LT-1 и LT-2), разветвитель при этом имеет тип 2xN (рис. 9). В случае повреждения основного волокна происходит автоматическое переключение на модуль LT-2 в центральном узле OLT с последующим восстановлением соединения после потери связи.

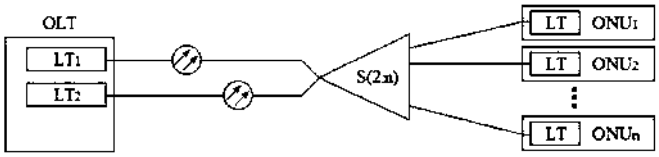

Рис. 9. Схема частичного резервирования со стороны OLT

Полное резервирование. Полное резервирование заключается в использовании запасных комплектов оконечных устройств OLT и ONU, волоконно-оптических линий, приемопередающих модулей, а также оптических разветвителей. Схема полного резервирования изображена на рис. 10. Восходящий поток, формируемый LT-1 и LT-2 со стороны абонентского узла ONU, передается по двум каналам связи. Центральный узел OLT обрабатывает продублированный сигнал и передает на магистраль одну копию сигнала. Передача нисходящего потока происходит аналогичным образом.

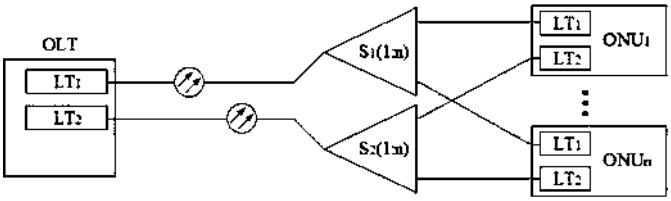

Рис. 10. Схема полного резервирования

В случае отказа приемопередающего оборудования или повреждения оптической линии возможно своевременное переключение на резервные устройства и компоненты сети без прерывания связи. При полном резервировании сети PON обладают наибольшей живучестью, однако для реализации полного дуплекса требуются огромные материальные затраты.

Частичное резервирование со стороны ONU. Этот метод аналогичен предыдущему с той разницей, что резервированию могут подвергаться не все оконечные устройства ONU, а лишь часть из них. В случае резервирования узлы ONU оборудуются двумя приемопередающими модулями LT-1 и LT-2, а в случае отсутствия резервирования – модулем LT. На рис. 11 приведена схема частичного резервирования со стороны ONU. Процесс переключения на резервный модуль LT-2 с активного модуля LT-1 осуществляется аналогично как на центральном узле OLT.

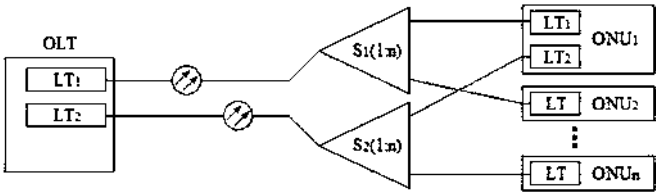

Рис. 11. Схема частичного резервирования со стороны ONU

Заключение

Для обеспечения живучести сетей PON необходимы комплексные меры предполагающие контроль доступа к ресурсам сети (информации и оборудованию), а также сохранение целостности данных при их хранении и передаче через сеть. В базовый функционал защиты сетей PON должны входить [3]: процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. д.

Живучесть сетей связи может быть повышена путем принятия комплекса инженерно-технических и организационных мер. К таким мерам относятся [5]: выбор структур, обладающих повышенной живучестью; введение в систему структурной и функциональной избыточности; повышение удельного веса в системе более устойчивых линейных средств и защита станционных сооружений узлов. Выбор структур, обладающих повышенной живучестью, осуществляется путем сравнения характеристик живучести различных топологий сети. В сетях PON информация между абонентами или сегментами сетей проходит через линейный терминал OLT. В таком случае наличие лишь одного канала связи может при нарушении функционирования центрального узла OLT вывести из строя целый сегмент сети PON. Для предотвращения подобных ситуаций необходимо применять различные методы резервирования каналов связи и оконечного оборудования.

Литература

1. *Птицын Г.А.* Живучесть динамических сетей телекоммуникаций / Под ред. Петракова А.В.: Учебное пособие. – М.: МТУСИ, 2008. – 48 с.

2. *Птицын Г.А.* Живучесть динамических сетей связи / Под ред. Петракова А.В.: Учебное пособие. – М.: МТУСИ, 2008. – 98 с.

3. *Алексеев Е.Б.* Оптические сети доступа. Учебное пособие – М: ИПК при МТУСИ, 2005 г. – 140 с.

4. *Птицын Г.А.* Живучесть сетей сообщений. Учебное пособие. – М.: МТУСИ, 2001. – 54 с.

5. Надежность и живучесть систем связи / Под ред. Дудника Б.Л. – М.: Радио и связь, 1984. – 216 с.