Развитие и безопасность пассивных оптических сетей

Для поддержки бурного роста Интернет-трафика технология пассивных оптических сетей (PON) кажется идеальным решением, которое стремительно внедряется во всем мире. Рассматриваются развитие технологии PON и аспекты её информационной безопасности.

Бирин Д.А.

С появлением все новых сервисов для пользователей Сети, происходит бурный рост трафика. По данным прогноза Cisco Virtual Networking Index [1] (июнь 2010 г.), в 2013 году в Сети будет ежемесячно передаваться объем информации, измеряемый 10 миллиардами DVD-дисков. 90% этой информации будет составлять видео, а на его просмотр в режиме реального времени понадобится 500 тысяч лет, рис. 1.

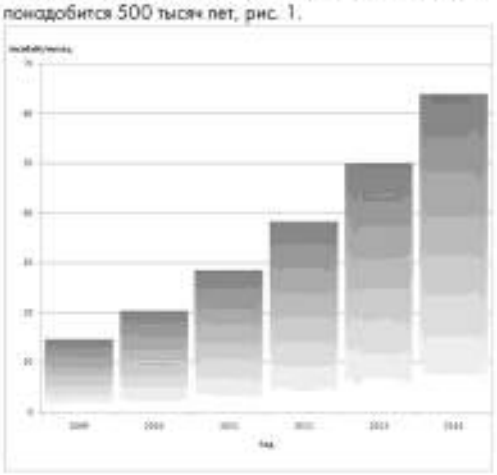

Рис. 1. Прогноз роста интернет-трафика в экзабайтах в месяц

Потоковое видео вместе с файлообменом уже в настоящее время составляет большую часть Интернет-трафика, а 2010 год во многих странах по прогнозам Cisco станет переломным, - когда трафик видео превысит трафик обмена файлами. В России, в связи с популярностью P2P сетей, этот момент прогнозируется на 2011-2012 годы. Для поддержки такого бурного роста трафика технология пассивных оптических сетей (PON) кажется идеальным решением.

Решения на основе архитектуры PON используют логическую топологию "точка-многоточка". К одному порту центрального узла можно подключать целый волоконно-оптический сегмент древовидной архитектуры, охватывающий десятки абонентов. Пассивные оптические сети состоят из оптического станционного терминала OLT, пассивных оптических разветвителей (сплиттеров) и оптического сетевого абонентского терминала/устройства ONT/ONU, рис. 2.

Рис. 2. Пример пассивной оптической сети

Разработкой стандартов PON занимаются авторитетные стандартизующие организации Международный Союз Электросвязи (ITU) и Институт Инженеров Электротехники и Электроники (IEEE). Первые шаги в технологии PON были предприняты в 1995 г., когда влиятельная группа из семи компаний (British Telecom, France Telecom, Deutsche Telecom, NTT, KPN, Telefonica и Telecom Italia) создала консорциум для того, чтобы претворить в жизнь идеи множественного доступа по одному волокну. Эта организация поддерживаемая ITU, получила название FSAN (Full Service Access Network). Целью FSAN была разработка общих рекомендаций и требований к оборудованию PON для того, чтобы производители оборудования и операторы могли сосуществовать вместе на конкурентном рынке систем доступа PON.

Первым стандартом ITU стал APON (Asynchronous Transfer Mode (ATM) PON). Дальнейшим развитием PON является BPON (Broadband PON), основанный на стандарте APON с некоторыми улучшениями (ITU-T G.983), обеспечивая 622 Мб/с в нисходящем потоке и 155 Мб/с в восходящем. Следующим поколением стал стандарт ITU-T G.984 или GPON (Gigabit-capable PON), вступивший в силу в марте 2008 г. GPON обеспечивает до 2.488 Мб/с в направлении к абоненту и до 155 Мб/с от абонента.

В настоящее время ITU и FSAN разрабатывается еще одно поколение PON, так называемый NG-PON. Его разработка включает в себя две фазы: XG-PON и, собственно, NG-PON. Первая фаза фокусируется на поколении оптических сетей доступа, которые могут сосуществовать с существующей GPON-технологией. Вторая фаза нацелена на следующее поколение оптических сетей доступа, которые будут независимы от существующих технологий PON. Стандарт XG-PON1 (ITU-T G.987) был утверждён в июне 2010 г. и предос-

тавляет абонентам 10 Гб/с в нисходящем и 2,5 Гб/с в восходящем потоках. В ноябре Portugal Telecom и Huawei провели первые полевые испытания сети стандарта XG-PON1 в Европе [2]. А американская компания Verizon проводила похожие тесты ещё летом 2010 г. [3].

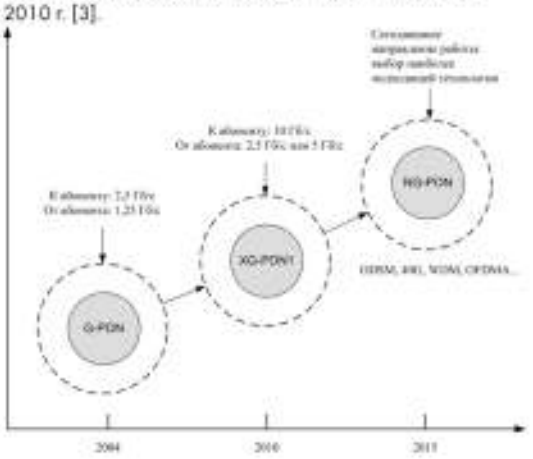

Рис. 3. Эволюция стандартов ITU-T по PON

Со стороны IEEE в 2004 г. в стандарте IEEE 802.3ah («Ethernet на последней миле») был описан стандарт EPON, использующий PON для передачи Ethernet-кадров. EPON поддерживает 1 Гб/с как в восходящем, так и в нисходящем направлениях. В сентябре 2009 г. был утверждён стандарт IEEE 802.3av, описывающий стандарт нового поколения — 10G-EPON. Как видно из названия, он как и XG-PON поддерживает скорость нисходящего потока до 10 Гб/с. Одни из первых полевых испытаний технологии в мае 2010 г. были проведены компанией ZTE [4].

И EPON и GPON имеют свои преимущества и недостатки, подробно описанные в статьях [5]. К примеру, GPON может предложить более высокую скорость и более эффективно использует полосу пропускания, тогда как EPON более эффективен экономически и в нём лучше организована поддержка IPTV.

Пассивные оптические сети многими считаются довольно безопасной технологией с точки зрения несанкционированного доступа по двум причинам. Во-первых, PON используют в качестве физической среды передачи данных оптоволокно, имеющее высокую степень защищенности информации от несанкционированного доступа, чем иная среда передачи данных, что связано с физическими принципами распространения электромагнитной волны в световоде. В оптическом волноводе электромагнитное излучение выходит за пределы волокна на расстояние не более длины волны при отсутствии внешнего воздействия на оптоволокно. Т.е. для попытки несанкционированного доступа нужен физический контакт с оптоволокном. Во-вторых, PON является широковещательной технологией и для предотвращения доступа одного абонента к информации другого и в EPON и в GPON используется шифрование по криптостойкому алгоритму AES. Тем не менее, проблема информационной безопасности остается актуальной.

Рассмотрим основные виды несанкционированного доступа в пассивных оптических сетях [6]:

– «Нарушение услуги» или DoS-атака (denial of service). Данный вид несанкционированного воздействия может быть реализован через оптическое волокно или приемопередающее оборудование на стороне абонента (ONU/ONT) либо через оптический разветвитель. Простейшая атака такого типа состоит в использовании неисправного или специально изменённого лазера ONU, для того, чтобы постоянно передавать на длине волны от ONU злоумышленника к OLT сигнал достаточной мощности, и «глушить» остальные ONU. Так как сеть пассивна, то обнаружить ONU, вызвавший отказ достаточно сложно.

– «Подслушивание» может быть реализовано злоумышленником путем ответвления части оптической мощности передаваемого оптического сигнала через ОВ или оптический разветвитель. Данный вид воздействия можно применить двумя способами: разрывным или безразрывным. В случае разрывного способа производится обрыв оптического волокна и подсоединение оптического ответвителя. Несовершенство этого способа заключается в большом вносимом затухании и неизбежном прерывании связи на время подключения ответвителя, что может быть легко обнаружено. В случае безразрывного способа часть оптической мощности можно получить в месте изгиба оптического волокна. В настоящее время на рынке представлен целый ряд оптических телефонов, которые позволяют организовать связь на дальних расстояниях по оптическому волокну без нарушения целостности последнего при помощи "оптических прищепок". "Оптическая прищепка" за счет изгиба волокна позволяет как вводить, так и выводить оптический сигнал. На рынке предлагается целый ряд таких устройств стоимостью менее 1000 долл. с различными значениями вносимого затухания. Кроме того, на рынке представлены устройства, которые позволяют обнаружить наличие сигнала в оптическом волокне, определить его направление и поляризацию. Но как же быть с шифрованием?

Учёные из Стендфордского Университета в США нашли «лазейку» [7] в действующих стандартах PON. К примеру, по стандарту GPON необходимым считается шифрование только нисходящего потока, а решение о шифровании потока от абонента кладётся на плечи производителей и является необязательным, так как поток от абонента итак считается защищённым. Кроме того, в потоке от абонента могут передаваться ключи, которые можно использовать для дешифровки данных, получаемых абонентом. Коллеги из США провели ряд экспериментов на тестовом стенде и показали возможность доступа к данным передаваемым оконечным оборудованием жертвы подслушивания.

Таким образом, чтобы обеспечить полную безопасность сети от несанкционированного доступа, требуется шифрование и восходящего потока. Но любое шифрование понижает эффективность сети. Следовательно для сохранения эффективности PON нужно искать новые способы защиты информации и борьбы с несанк-

ционированным доступом, либо искать методы более эффективного использования ОВ.

Технология пассивных оптических сетей - ясное, довольно простое и экономически эффективное решение «проблемы последней мили». Оно стремительно внедряется во всём мире. И, как часто бывает с любой быстроразвивающейся технологией, её экономическая выгода ставит на второй план вопросы информационной безопасности. По нашему мнению, информационная безопасность PON требует серьезного исследования.

Литература

1. Cisco Visual Networking Index // Cisco Systems Inc. URL: http://www.ciscovni.com/vni_forecast/index.htm.
2. Впервые в Европе Portugal Telecom и Huawei проводят совместное тестирование услуг IPTV Meo и 3DTV с использованием технологии 10G-GPON// Huawei Technologies URL: http://www.huawei.com/ru/catalog.do?id=4422.
3. Implementing Next-Generation Passive Optical Network Designs with FPGAs // Altera Corporation. URL: http://www.altera.com/literature/wp/wp-01143-next-gen-pon.pdf.
4. «ZTE Announces Successful 10G EPON Testing in U.S. Market» // ZTE Corporation URL: http://wwwen.zte.com.cn/en/press_center/news/201005/t20100513_184642.html.
5. **Гладышевский М.А.** Сравнение технологий EPON и GPON // Lightwave Russian Edition. – 2005. – №2. – С.16-22.
6. **Буловкин И.А.** Вопросы информационной безопасности сетей PON // Технологии и средства связи. – 2006. – №2. – С. 104-108.
7. TDM-PON Security Issues: Upstream Encryption is Needed / David Gutierrez, Jinwoo Cho, Leonid G. Kazovsky // Optical Fiber Communication and the National Fiber Optic Engineers Conference, Анахайм, Калифорния, США, 25-29 Марта 2007.