ШИФРОВАНИЕ ДАННЫХ И ВОЛНОВОЕ УПЛОТНЕНИЕ КАНАЛОВ в магистральной сети

А.Куницкий, ведущий инженер компании "Ай-Теко"

Рассматривая актуальную проблему обеспечения безопасности информации при передаче по каналам связи, автор раскрывает возможности интересного сочетания технологий волнового уплотнения и шифрования в одном устройстве для решения нестандартных инженерных задач. В статье описываются ключевые технические особенности и экономические преимущества использования новых модулей на примере продуктовой линейки оборудования Cisco.

Обзор решения

Совмещение в одном оборудовании двух технологий – шифрования данных и волнового уплотнения каналов (DWDM, Dense Wavelength-Division Multiplexing) – необычная инженерная задача и интересное сочетание технологий.

Первая причина, обусловившая возникновение данной задачи, – необходимость защиты информации. Проблема обеспечения безопасности данных возникла при появлении информации, которую надо защитить от посторонних глаз. Если ранее данные хранились на физических носителях (бумаге, фотопленке, магнитных носителях) и для обеспечения их сохранности использовались стандартные средства – сейфы и охраняемые помещения, то с приходом века информационных технологий ситуация кардинально изменилась. Все больше информации хранится и передается в электронном виде. Злоумышленникам теперь не надо взламывать сейфы и проникать на охраняемую территорию, им всего лишь нужно получить доступ к телекоммуникационной сети, по которой пересылается конфиденциальная информация. Для предотвращения подобных неправомерных действий государственными контролирующими органами разрабатываются и совершенствуются регламенты, правила и требования к защите передаваемых данных.

Для коммерческих банков контролирующими органами, которые регламентируют использование, ввоз и получение лицензий на оборудование с функциями шифрации, выступают Банк России и ФСБ. Согласно регламентам, необходимо использовать шифрование для защиты персональных данных, однако Банк России не выдвигает конкретных и детальных требований по выбору технических или организационных мер. Участники Национальной платежной системы вправе самостоятельно определять средства защиты. Требований по применению сертифицированных средств защиты информации в коммерческих банках нет [1].

Из-за большого количества юридических тонкостей вопрос безопасности персональных данных заслуживает отдельной статьи. Мы сосредоточимся лишь на технической части. На территории организации, работающей с персональными данными, защиту каналов связи можно обеспечить путем ограничения доступа к местам прокладки

информационных кабелей. Но для каналов, выходящих за территорию организации, это сделать практически невозможно. Тут-то и возникает задача шифрования трафика, проходящего по магистральным каналам.

Вторая причина – увеличение объемов передаваемой информации. На коротких расстояниях обычно не составляет труда организовать несколько каналов связи между оборудованием, что достигается прокладкой дополнительных соединительных линий. Однако на больших расстояниях в городских и региональных сетях это может быть проблематичным. Прокладка дополнительных оптических волокон стоит довольно дорого. Кроме того, значительное затухание сигнала на протяженной линии может не позволить соединить оборудование напрямую. В этом случае неоспоримым преимуществом становится применение DWDM – технологии спектрального волнового уплотнения каналов.

Для решения каждой задачи – шифрования и уплотнения – можно использовать отдельное оборудование, и сначала шифровать данные на одном оборудовании, а затем уплотнять на другом. Компания Cisco создала комплексное решение, которое объединяет эти две технологии и включает в себя DWDM-платформу с возможностью шифрования трафика и программное обеспечение, позволяющее в полной мере обеспечить безопасность передачи информации.

SMART: "умное" поколение оборудования

Рассмотрим технические характеристики платформы в целом и платы в отдельности, а также сценарии использования данного оборудования.

При создании NGN (Next Generation Networks, New Generation Networks – сети следующего/нового поколения) DWDM-системы компания Cisco ориентировалась на оптимизацию рабочих процессов пользователей DWDM-систем и фокусировалась на создании автоматизированной системы нового поколения – сокращенно SMART:

- Simplified: простая эксплуатация, по аналогии с оборудованием SDH;
- Multi-purpose: единая система для решения разных задач;
- Automated: интеллектуальный контроль уровней мощности с перенастраиваемыми оптическими модулями и интерфейсами;
- Reliable: система операторского класса с соответствующим уровнем отказоустойчивости;
- Transport: платформа, позволяющая предоставлять качественный и надежный транспорт для любых сервисов.

Платформа Cisco ONS 15454 MSTP позволяет эффективно решать задачи растущего спроса на мультисервисные услуги, увеличения пропускной способности, обеспечения гибкости сети, преодоления больших расстояний и обеспечения простоты управления. Платформа поддерживает создание DWDM-сетей как самой простой топологии "точка-точка", так и сложных разветвленных топологий с кольцевым резервированием, вплоть до полносвязных "ячеистых" топологий. Каждый узел может быть сконфигурирован как терминальный, как линейный усилитель, как узел ввода-вывода, в том числе перенастраиваемый (ROADM, Reconfigurable Optical Add-Drop Multiplexer). Все это разнообразие возможно благодаря большому количеству модулей: оптических фильтров, оптических усилителей, транспондеров, мукспондеров и других вспомогательных модулей. Широкий выбор мультиплексоров ввода/вывода позволяет организовать вывод от 1 до 96 оптических каналов. Наличие перенастраиваемых мультиплексоров ввода/вывода (ROADM) позволяет сконфигурировать на узле до 16 оптических направлений. За счет использования передовых разработок в области когерентного детектирования и технологий коррекции ошибок, а также применения улучшенных эрбиевых и рамановских оптических усилителей, возможно передавать сигнал на расстояния до 5000 км без промежуточного O-E-O-преобразования. Встроенное измерение оптических параметров в контрольных точках позволяет контролировать состояние сети в каждый момент времени и своевременно реагировать на изменения.

Мощная система планирования и моделирования DWDM-сети Cisco Transport Planner (CTP) позволяет заранее просчитать все параметры сети и выбрать наиболее подходящие конфигурации оборудования. Интегрированная система управления Cisco Transport Controller (CTC) помогает быстро вводить новые узлы в эксплуатацию. Интеллектуальная система управления Cisco Transport Management (CTM) обеспечивает автоматическое управление оптическими параметрами сети, сквозную активацию каналов, корреляцию аварий на уровне сети и много других функций. Платформа Cisco ONS 15454 MSTP предоставляет богатый набор инструментов, позволяющих строить интеллектуальные сети NGN DWDM.

Шасси и карты

В данной платформе представлено три типа шасси – M12, M6 и M2 (рис.1). Количество слотов, доступных для карт обработки и передачи трафика, заложено в название шасси. В шасси M12 – 12 слотов, в M6 и M2 – соответственно 6 и 2 слота. Остальные слоты

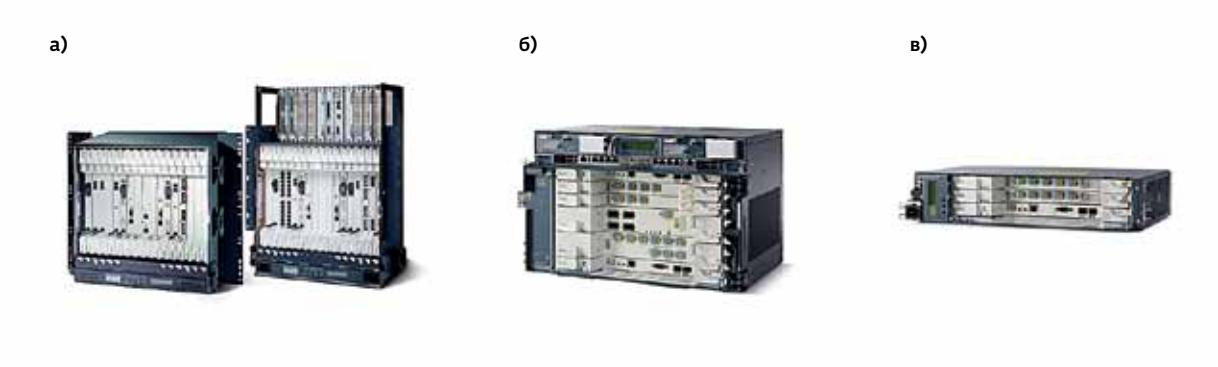

Рис.1. Основные типы шасси: а) шасси M12 (слева форм-фактор ANSI, справа – ETSI), б) шасси M6, в) шасси M2

зарезервированы под карты управления, карты служебного канала связи и вывода аварий. Блоки питания, управляющая карта и вентиляторы в шасси M12 и M6 зарезервированы. В шасси M2 управляющая карта и блок питания не резервируются [2]. Большое разнообразие карт и их функциональности (см. таблицу) позволяет сконфигурировать систему под любые задачи [3]. Карта WSE (рис.2) добавила к этому списку возможность шифрования трафика.

Ключевые функции карты шифрования WSE

Карта WSE (Wire Speed Encryption) позволяет шифровать данные на OTN-уровне, соответствующем уровню L1 в модели OSI. Данная карта разработана для использования на платформе Cisco ONS 15454 MSTP и поддерживается, начиная с версии программного обеспечения 9.8. На карте расположено десять портов для установки модулей SFP+ (скорость до 10 Гбит/с), которые могут быть сконфигурированы и как клиентские, и как линейные интерфейсы. Можно каждый порт сконфигурировать отдельно и отправить данные с него как на шину данных, так и на соседний порт.

На клиентских портах карты WSE поддерживаются следующие типы интерфейсов: 10GE LAN PHY, OTU2, OTU2e, STM-64 и Fiber Channel. Линейные DWDM-порты могут быть перенастроены на 96 длин волн с шагом 50 ГГц в C-диапазоне. Формат DWDM-сигнала соответствует стандарту ITU-T G.709, что позволяет настраивать передачу служебных данных GCC, включать коррекцию ошибок FEC либо расширенную коррекцию ошибок EFEC и собирать статистическую информацию.

Рис.2. Внешний вид карты WSE

Плата обеспечивает целостную и конфиденциальную передачу данных по оптоволоконному каналу связи благодаря шифрации нового поколения. Надежность архитектуры всей системы обеспечивается соответствием стандарту FIPS 104-2. Стандарт FIPS (Federal Information Processing Standard) публикации 140-2 разработан Американским национальным институтом стандартов (NIST) и определяет требования, которым должны соответствовать криптографические модули [4].

Карта WSE может быть настроена на несколько режимов работы. Выбор зависит от дизайна сети. Поддерживается режим транспондера, регенератора либо их комбинация. Карта может быть оснащена клиентскими и линейными модулями SFP+. В ходе первоначальной загрузки происходит проверка на аппаратном уровне, гарантирующая, что только подлинное программное обеспечение Cisco загрузится на платформу Cisco. Данная функция предотвращает несанкционированное вмешательство и клонирование ПО при загрузке. Цифровая подпись гарантирует, что образ программного обеспечения, работающего на устройствах Cisco, подлинный. При этом сохраняется целостность образа, который загружается на WSE-карты. Обмен ключами между надежными картами происходит через служебный канал связи GCC2, который защищается с помощью протокола TLS (Transport Layer Security). Для обмена ключами используется алгоритм ECDHE (Elliptic Curve Diffie Hellman Ephemeral). WSE-карта

Основные параметры мультисервисных карт

Карта	Количество занимаемых слотов	Емкость, Гбит/с	Порты	Сервисы
10DME-C	1	10	8 клиентских SFP 1 линейный перенастраиваемый	GE, 1/2/4G FC/FICON
4×2.5G Muxponder	1	10	4 клиентских SFP 1 линейный перенастраиваемый	STM-16
OTU2-XPonder	1	20	2 клиентских XFP 2 линейных XFP перенастраиваемых	STM-64, 10GE LAN/WAN, 10G FC, OTU2
MSPP-on-Blade	2	20	16 клиентских SFP 3 линейных XFP перенастраиваемых	STM-1/4/16,STM-64, GE
GE-Xponder	2	20	20 клиентских SFP 2 линейных XFP перенастраиваемых	10/100/GE, 10GE
Any Rate-Xponder	1	40	10 клиентских или линейных SFP и XFP перенастраиваемых (все порты G.709)	STM-1/4/16/64, OTU1/2, 1/10/100/GE, 10GE LAN/WAN, 1/2/4/8/10G FC, SD/HD Video
40G Coherent TXP	2	40	1 клиентский 1 перенастраиваемый линейный	STM256, OTU3, 40GE CBR
40G Coherent MXP	2	4×10	4 клиентских XFP 1 перенастраиваемый линейный	8G/10G FC, 10GE LAN/WAN, STM64, OTU2
40G Coherent Metro TXP	2	40	1 клиентский 1 перенастраиваемый линейный	STM256, OTU3, 40GE CBR
40G Coherent Metro MXP	2	4×10	4 клиентских XFP 1 перенастраиваемый линейный	8G/10G FC, 10GE LAN/WAN, STM64, OTU2
100G Coherent MXP	1	100	1 клиентский CXP 1 перенастраиваемый линейный	100GE, OTU4
10×10G	1	100	10×SFP + шина	10GE, STM64, OTU2
2×CFP	2	200	2xCFP	100GE CFP
WSE	1	100	10×SFP + шина	10GE LAN/WAN, OTU2

GE – Gigabit Ethernet, FC – Fiber Channel

защищает от манипуляций с зашифрованными данными и манипуляций типа "вырезать-вставить". В режиме работы XTS (Xor-Encrypt-Xor Encryption Mode with Tweak and Ciphertext Stealing) используется алгоритм AES-256. Управление транспортными функциями и функциями безопасности полностью разделено в системе управления. Как результат – пользователь может выполнять только разрешенные ему операции, в зависимости от назначенной роли. Сертификат SUDI (Secure Unique Device Identification) соответствует стандарту IEEE 802.1AR. Подписанный с помощью Cisco's Root Certificate Authority, он содержит уникальный идентификатор, который используется для проверки подлинности карты WSE перед обменом данными. Информация не может быть передана на карту, которая не прошла проверку подлинности. Карты WSE поддерживают GCC-каналы (General Communication Channel) на клиентских и линейных портах OTN (OTU2/OTU2e). Может быть сконфигурировано до десяти каналов GCC0 и до пяти GCC1/2 на платформе Cisco ONS 15454 MSTP. Можно организовать защиту DWDM-сигнала за счет внешнего модуля PSM (Protection Switch Module). Лицензирование карты предлагает экономически эффективное решение для клиентов, которым не требуется на начальном этапе шифрование данных на всех портах [5].

Сценарии

Имея представление о возможностях платформы Cisco ONS 15454 MSTP и карты WSE, поговорим о сценариях ее использования.

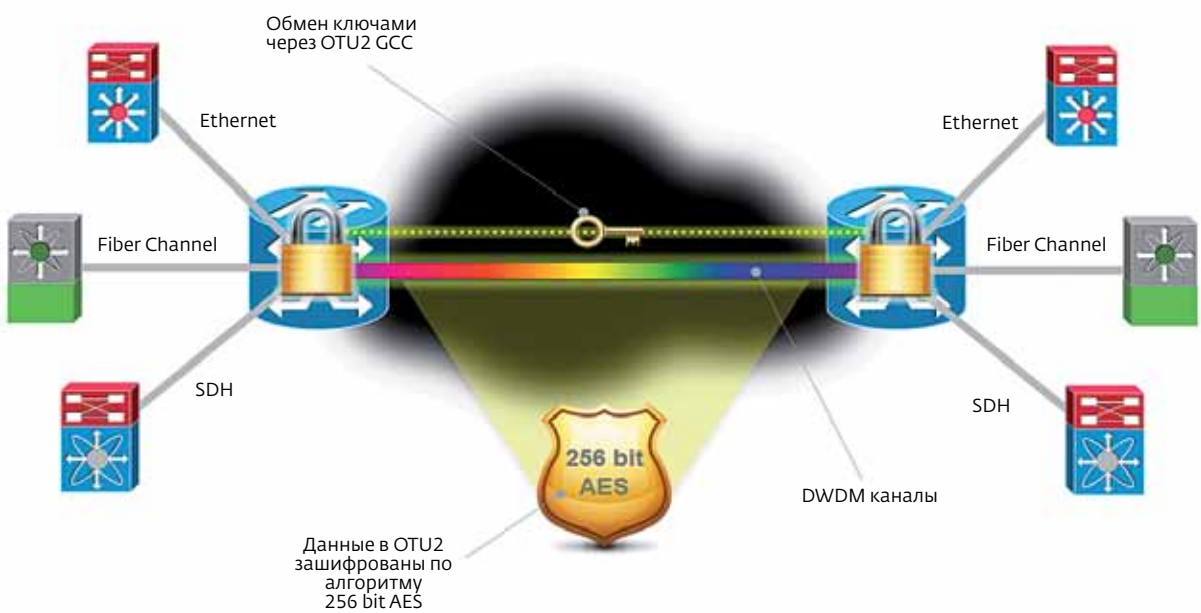

Рис.3. Типичная архитектура сети

Основные потребители данного решения – коммерческие банки. У большинства крупных банков есть несколько центров обработки данных (ЦОД) и несколько офисов, расположенных в пределах города, страны или даже мира. Между этими объектами необходимо передавать большие объемы информации для синхронизации баз данных, пересылки внутренних документов, работы внутренней сети банка и т.д. По существующим нормативам, банкам необходимо шифровать весь трафик, содержащий персональные данные. Самый надежный способ – установить оборудование шифрования на внешних каналах связи. Существует узкоспециализированное оборудование, которое выполняет функцию только шифрования данных. Но в большинстве случаев у банка есть несколько параллельных систем, обменивающихся информацией по разным интерфейсам. Например, системы хранения данных чаще всего обмениваются по интерфейсу Fiber Channel, а внутренние компьютерные сети построены на технологии Ethernet. Встречаются и традиционные телефонные сети, передающие информацию через сеть SDH (Synchronous Digital Hierarchy).

Для каждой из этих технологий придется прокладывать или арендовать отдельную пару волокон или использовать систему DWDM, озаботившись вопросами шифрования каждого типа трафика.

Предложенное компанией Cisco решение (рис.3) на базе Cisco ONS 15454 MSTP и карты WSE позволяет решить все эти проблемы в рамках одной платформы с единым управлением и контролем. В текущей версии программного обеспечения карта WSE поддерживает шифрование трафика 10GE и OTU2 (рис.4), но в следующей версии ПО будут реализованы

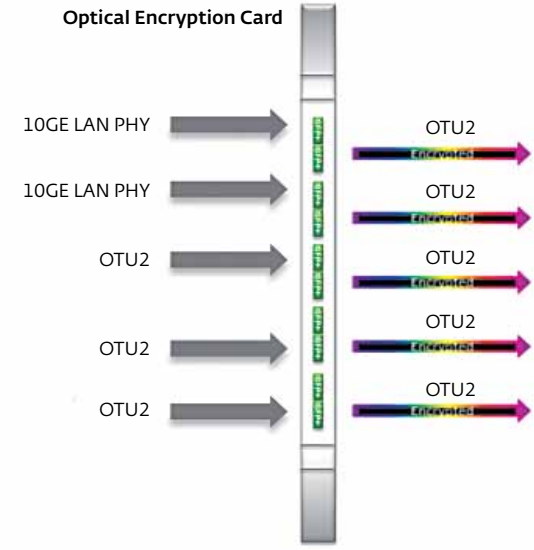

Рис.4. Карта WSE

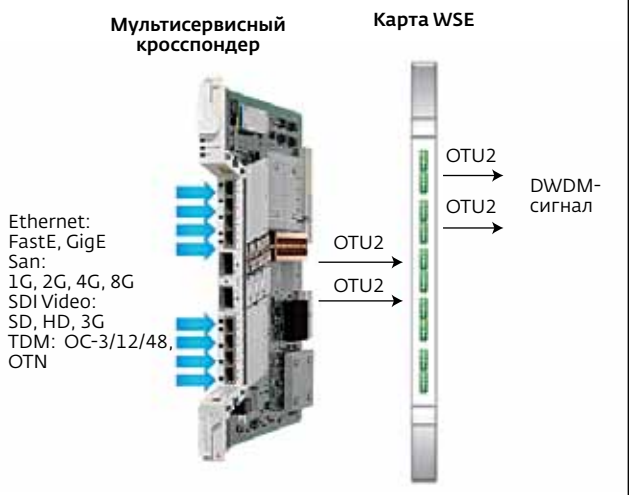

Рис.5. Карта WSE и мультсервисный кросспондер

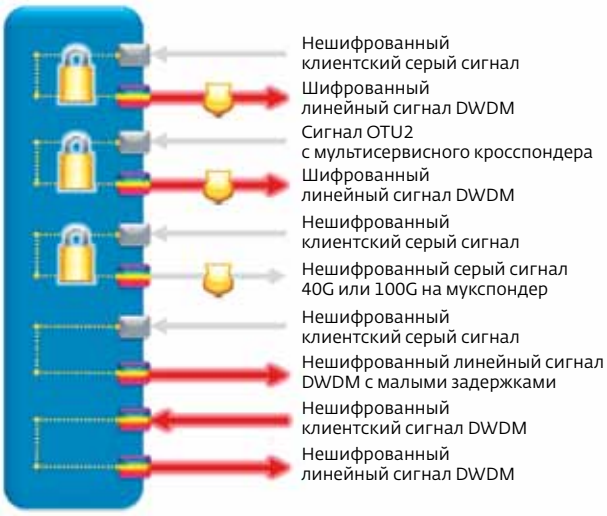

Рис.6. Варианты настройки портов карты WSE

и остальные протоколы, включая STM-64, 8G и 10G Fiber Channel, FICON (Fibre Connection). Если необходимо обеспечить шифрование данных для менее быстрых интерфейсов, то с помощью мультисервисного мультиплексирующего кросспондера можно собрать разные виды трафика (FC, GE, SDH и т.д.) в сигнал OTU2, который потом зашифруется картой WSE (рис.5). Таким же образом карта WSE может быть сконфигурирована со многими другими транспондерами и мукспондерами. Например, можно зашифровать десять потоков по 10 Гбит и, собрав их в OTU4, передать по одному 100-гигабитному каналу DWDM. Шифрации подвергается только сам блок данных, а OTU2 можно легко передать через сети сторонних операторов и вывести в любой точке мира. Для подключенного оборудования это будет выглядеть как прямое соединение.

Часто к каналам для синхронизации систем хранения данных предъявляют жесткие требования по задержкам сигнала, карта WSE полностью соответствует им. Шифрация происходит на уровне OTU стандарта G.709, что соответствует уровню L1 модели OSI. Шифруется только блок данных, а сам контейнер и содержащаяся в нем служебная информация остаются неизменными. Так как информация передается контейнерами одинакового размера и с точно определенной периодичностью, это позволяет шифровать трафик без потери скорости канала. Вносимые задержки несущественны по сравнению с задержками, вызванными дальностью передачи.

У данной карты имеется существенный плюс, связанный с лицензированием. В базовой комплектации лицензированная карта WSE включает в себя шифрование одного потока. На карте WSE каждый порт конфигурируется независимо, и на начальном этапе, когда клиенту необходимо только несколько каналов с шифрацией, он может не платить за шифрацию на всех портах, а купить лицензию только на то количество, которое ему нужно (рис.6). Лицензированию подлежат только функции безопасности. WSE-карта без лицензии действует как простой транспондер/регенератор.

Подводя итоги, можно отметить многочисленные достоинства предлагаемого решения по шифрованию и уплотнению данных. Шифруются как сами данные, так и передаваемые ключи. Задержки передачи сигнала крайне малы. Система управления имеет разграничение прав доступа на управление транспортными функциями и функциями шифрования. Можно зашифровать большое количество типов сервисов. Предусмотрена гибкая система лицензирования количества портов с шифрованием.

ЛИТЕРАТУРА

1. IS_track: Чего ждать от регуляторов в ближайшее время? – http://www.cisco.com.
2. Обзор платформы Cisco ONS 15454 MSTP – http://www.cisco.com.
3. Cisco ONS 15454 DWDM Configuration Guide – http://www.cisco.com.
4. Cisco Optical Encryption Card – http://www.cisco.com.
5. Encrypted Transport Solutions, http://www.cisco.com.