

УДК 621.391

К.М. Руккас, К.А. Овчинников, Н.А. Королюк

*Харьковский национальный университет радиоэлектроники, Харьков***СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ УПРАВЛЕНИЯ СЕТЯМИ MPLS**

Приведены основные требования к системам управления сетью MPLS. Приведен обзор возможностей современных программных продуктов различных производителей, реализующих функции управления сетью MPLS с указанием особенностей архитектуры, методов и протоколов сбора и обработки статистической информации, системных требований и поддерживаемых платформ. Проведен сравнительный анализ возможностей существующих систем управления относительно требований международных стандартов ITU и IETF. Выявлено отсутствие механизмов динамического управления сетью и значительное несоответствие требованиям, выдвигаемым к сетям MPLS.

Ключевые слова: система управления сетью, мультипротокольная коммутация по меткам, простой протокол управления сетями.

Введение

Современные телекоммуникационные сети (ТКС) представляют собой сложные территориально распределенные многоуровневые системы, функционирующие по множеству протоколов и ориентированные на предоставление широкого спектра мультимедийных услуг различной сложности. Эффективность ТКС зависит от множества параметров, таких как показатели качества обслуживания, надежности, производительности, экономичности, и др., в то же время значение всех этих показателей может значительно варьироваться в зависимости от текущей загрузки сети. Из этого следует, что в большинстве случаев для обеспечения эффективного функционирования ТКС необходима автоматическая система управления (АСУ), способная отслеживать текущее состояние сети и вносить корректировки в ее работу с целью повышения эффективности. Также важной задачей разработки АСУ является минимизация воздействия человеческого фактора на решение задач управления, что выражается в таких требованиях, как адаптивность и обучаемость.

1. Общие требования к АСУ ТКС

Ключевые функции администрирования и управления телекоммуникационными сетями отражены в модели Международной организации по стандартизации, описанной в стандартах М.3010 и М.340. Широкое распространение получила аббревиатура FCAPS, отражающая задачи, которые должна решать АСУ ТКС:

- (F) Fault Management (управление отказами);
- (C) Configuration Management (управление конфигурацией);
- Accounting Management (учёт);
- (P) Performance Management (управление производительностью);
- (S) Security Management (управление безопасностью).

К основным задачам, которые должна решать АСУ ТКС на основе MPLS, относятся [3]:

- мониторинг состояния LSP;
- мониторинг конфигурации сети;
- измерение уровня качества обслуживания;
- определение и устранение неисправностей;
- сбор статистики о трафике;
- идентификация DoS-атак.

Все эти функции должны быть автоматизированы, АСУ должна поддерживать стандартные протоколы управления и формат MIB, описанный в RFC 3813. Каждый производитель оборудования использует свои библиотеки MIB, представляющие собой расширенные стандартизированные IETF библиотеки для MPLS MIB. Эффективность СУ в данном конкретном случае зависит от наличия в ней специализированных библиотек различных производителей оборудования, что обеспечивает аппаратную независимость и расширение возможностей СУ.

2. Современные АСУ MPLS

Ниже приведен анализ возможностей современных АСУ MPLS от различных разработчиков.

2.1. Cisco MPLS Management Essentials

Cisco MME – совокупность программных продуктов для организации управления сетью MPLS. В Cisco MME входят:

- IP Solution Center – планирование, управление ресурсами, поиск неисправностей;
- Cisco Prime LAN Management Solution (LMS) – управление инфраструктурой;
- Cisco Info Center – сбор и обработка статистической информации.

Cisco MME использует централизованную платформенную архитектуру.

Максимальная производительность программного продукта достигается при работе с оборудованием Cisco, что обуславливается наличием в IOS (операционной системе маршрутизаторов Cisco)

дополнительных функций, разработанных компанией Cisco.

IP Solution Center – центральная составляющая системы управления. В него входят: модуль диагностики VPN (обнаружение и анализ неисправностей на основе заложенных разработчиком сценариев) и модуль создания и анализа состояния VPN (создание и использование шаблонов для различных сервисов, резервирование полосы пропускания).

Cisco Prime LAN Management Solution – дополнительный модуль Cisco MME для мониторинга, обработки ошибок и планирования сетей MPLS, построенных исключительно на оборудовании Cisco. Может быть установлен отдельно от ISC. Мониторинг осуществляется при помощи протоколов SNMP и CDP (Cisco Discovery Protocol) путем циклического опроса всех узлов сети, при чем пользователю предоставляется возможность самостоятельного создания полей в MIB маршрутизатора и сценариев мониторинга. Максимально доступное количество обслуживаемых устройств на одном сервере – 5000. Поддерживаемые операционные системы: Solaris и Windows.

Cisco Info Center (CIC) – средство сбора, анализа и визуализации статистических данных, позволяющая оценивать производительность сети в целом. Программный продукт позволяет собирать и анализировать информацию уровня приложений. CIC минимальной комплектации содержит исключительно модуль анализа состояния сети передачи данных.

Системные требования: процессор UltraSPARC T2 x8, 16 Гб ОЗУ, 250Гб свободного места на жестком диске.

Поддерживаются операционные системы Windows Server, SUSE Linux, Linux Red Hat, IBM AIX, HP-UX, Solaris и RHEL.

2.2. Hewlett-Packard OpenView

HP OpenView – система мониторинга и управления ТКС от компании Hewlett-Packard. Продукт предлагается в двух версиях – Starter Edition и Advanced Edition. Версия Advanced Edition содержит модуль для работы с коммутируемыми сетями, поддерживает работу различных протоколов маршрутизации, содержит расширенный модуль диагностики устройств и сетей. В составе решения можно выделить два составляющих компонента:

- HP OpenView Network Node Manager – система мониторинга и управления сетями;
- HP OpenView Smart plug-ins – дополнительные специализированные программные модули, имеющие встроенные функции управления приложениями.

К основным функциям NNM можно отнести автоматический анализ топологии сети (используются протоколы SNMP и ICMP), графическое представление результатов мониторинга и анализа топологии сети, фильтрация отчетов об ошибках или недоступности оборудования. Условная схема архитектуры системы управления Network Node Manager представлена на рис. 1.

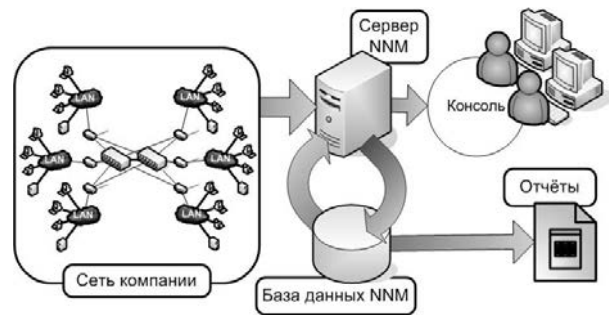


Рис. 1. Условная схема архитектуры системы управления Network Node Manager

Дополнительный модуль управления виртуальными частными сетями (Smart Plug-in for MPLS VPN) осуществляет мониторинг и предоставляет информацию о проблемах при диагностике отказа сети MPLS VPN. При обнаружении потери соединения, оператор получает необходимую информацию о клиентах и портах, на которых повлиял отказ.

В качестве отдельной АСУ выступает HP OpenView для сетей на оборудовании Juniper. Особенностью данной реализации является поддержка специальных полей MPLS MIB, разработанных и внедренных компанией Juniper.

Системные требования: процессор Intel Pentium4 и выше, 1 Гб ОЗУ, 8 Гб свободного места на жестком диске.

Программный продукт совместим с операционными системами Windows Server, Solaris и HP-UX.

2.3. ANMS SmartMIB

SmartMIB от Advanced Network Management Solutions Inc. – совокупность программных продуктов для мониторинга и управления телекоммуникационными сетями на основе протокола SNMP и модификаций HTTP. SmartMIB имеет одноуровневую архитектуру. В состав SmartMIB входят:

- SNMP MIB-браузер, позволяющий считывать или задавать значения полей MIB;
- модуль автоматического обнаружения оборудования, осуществляющий классификацию, инвентаризацию оборудования (осуществляется с помощью SNMP) и построение карты сети;
- модуль сбора, хранения и визуализации статистических данных, полученных с помощью SNMP;
- модуль обработки сообщений об ошибках, формирующий отчеты администратору сети.

Для работы с сетями MPLS необходим дополнительный модуль MPLS Management Bundle, позволяющий обрабатывать поля MPLS MIB, стандартизированные в RFC 3813. К ним относятся TE-тоннели, VPN-тоннели, состояние LSR и статистика интерфейсов LSR.

Системные требования: процессор Intel Pentium 4 и выше, 1 Гб ОЗУ, 1 Гб свободного места на жестком диске.

Совместимость: Microsoft Windows Server.

2.4. CA Spectrum

Spectrum от CA Technologies – система управления сервисами и устройствами, осуществляющая мониторинг состояния сетевых узлов, каналов связи, хост-систем и приложений. Как и остальные системы управления, Spectrum реализован с использованием архитектуры агент-менеджер: центральный элемент, SpectroSERVER, осуществляющий сбор статистики с помощью протокола SNMP, и клиентского приложения OneClic, позволяющее системному администратору взаимодействовать с сервером (рис. 2).

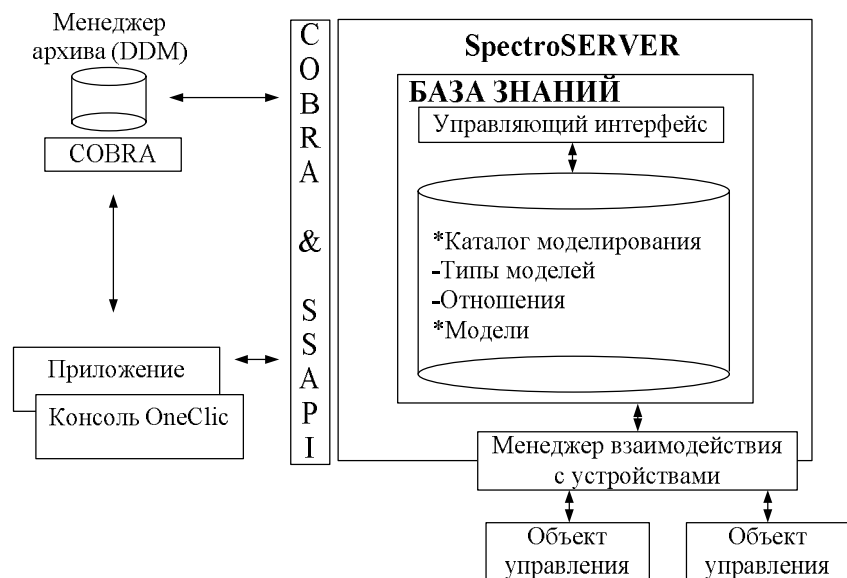


Рис. 2. Упрощенная схема взаимодействия компонентов SpectroSERVER

CA Spectrum представляет собой средство моделирования ТКС. Обнаружение устройств происходит при помощи протокола ICMP. После сбора всей необходимой информации СУ способна реализовать графическое представление физической и логической архитектуры сети. Ключевой функцией СУ Spectrum является средство моделирования поведения сети, что позволяет системному администратору обнаруживать потенциально слабые места сети и тестировать возможности развертывания новых сервисов. Для получения возможности получать отчеты о состоянии сети необходим отдельный самостоятельно лицензируемый модуль CA eHealth, осуществляющий мониторинг сети с помощью протокола SNMP и направляющий сообщения об ошибках системному администратору. В нем же содержатся средства мониторинга состояния MPLS VPN, отсутствующие в Spectrum.

Стандартные функции управления, а именно мониторинг состояния сети, сбор и хранение статистики и обработка сообщений об ошибках, собраны в отдельном модуле CA Unicenter NMS, имеющем иерархическую архитектуру. Unicenter также способен отслеживать выполнение SLA.

Системные требования: процессор UltraSPARC III x2 (Solaris) или Intel Pentium4 1.5 ГГц (другие ОС), 2,5 Гб ОЗУ, 2 независимых винчестера.

Поддерживаемые операционные системы: Windows, Linux Red Hat, SUSE Linux, IBM AIX, Sun Solaris, HP-UX.

2.5. EMC Ionix

Ionix от EMC – семейство программных продуктов, обеспечивающих мониторинг и анализ ТКС предприятия. В составе решения можно выделить следующие компоненты:

IP Availability Manager – средство мониторинга в режиме реального масштаба времени состояния узлов и каналов связи, содержащее в себе алгоритм определения первопричины неполадок;

Application Connectivity Monitor – используя средства IP Availability Manager позволяет идентифицировать причины ошибок приложений, связанные с недоступностью хоста, отказа сетевого компонента и другие ошибки, связанные с инфраструктурой сети;

IT Performance Reporter Network Edition – средство сбора и анализа статистики о производительности сети, предоставляющее системному администратору отчеты об «узких местах» и других потенциально слабых местах;

Service Assurance Manager – средство мониторинга качества предоставляемых услуг на основе статистической информации об интенсивности трафика и загрузки сети.

MPLS Manager – средство сбора и визуализации информации о топологии, путях коммутации меток (LSP) и виртуальных каналах (VPN) MPLS.

Отличительной особенностью Ionix является наличие модуля IT Operations Intelligence Third-Party Adapters, позволяющего взаимодействовать с СУ сторонних производителей (HP, Cisco и др.), что обеспечивает возможность мониторинга сложных распределенных неоднородных сетей.

Поддерживаемые платформы: Windows Server, Solaris, HP-UX, IBM-AIX и Linux Red Hat.

2.6. Dorado Software Redcell

Множество программных продуктов, разработанных под маркой Redcell компанией Dorado Software, обеспечивает решение задач мониторинга и анализа статистических данных о производительности ТКС. Аналогично ранее рассмотренным решениям, Redcell имеет модульную структуру. Центральный компонент, Redcell OpsCenter, осуществляет задачи автоматического определения топологии сети; мониторинга текущего состояния узлов и каналов связи; сбора, анализа и хранения статистической информации; визуализации полученной ин-

формации; оповещения системного администратора о возникших проблемах и предложения по их устранению. Дополнительно к Redcell OpsCenter можно установить множество модулей, основные из них:

Network Commander – модуль взаимодействия с фирменными операционными системами маршрутизаторов, повышающий эффективность мониторинга и расширяющий возможности статистического анализа;

Advanced Monitor – модуль анализа выполнения SLA, основан на специфических значениях MIB (поддерживается оборудование Cisco и Avaya);

Traffic Flow Analyzer – средство анализа трафика, передаваемого через управляемую сеть;

MPLS Module – дополнение, позволяющее отслеживать существующие LSP и создавать собст-

венные пути коммутации меток с резервированием ресурсов. Модуль также поддерживает мониторинг и создание MPLS VPN.

Поддерживаемые платформы: Windows Server, Solaris, Linux Red Hat, SUSE Linux.

Существует также множество менее популярных систем управления, например, OpManager, разработанный компанией AdventNet и OidView от ByteSphere. Эти системы построены на протоколе SNMP и их функциональность ограничивается возможностью сбора статистики о состоянии сети.

Заключение

В табл. 1 приведено сравнение рассмотренных решений в области управления сетями MPLS.

Таблица 1

Сравнительный анализ систем управления

| Производитель | Cisco | HP | ANMS | CA | EMC | Dorado | AdventNet | ByteSphere |
|----------------|-----------------------------|----------|----------|----------|-------|---------|-----------|------------|
| Название | MME | OpenView | SmartMIB | Spectrum | Ionix | Redcell | OpManager | OidView |
| FCAPS | + | ± | + | + | + | + | ± | ± |
| MPLS (RFC4377) | Мониторинг LSP | – | – | – | – | + | – | – |
| | Мониторинг структуры | + | + | + | + | + | + | + |
| | Мониторинг SLA | + | + | – | + | + | ±** | – |
| | Мониторинг VPN | + | + | + | + | + | – | – |
| | Регистрация ошибок | + | + | + | + | + | + | + |
| | Автомат. исправление ошибок | – | – | – | – | – | – | – |
| | Статистика трафика в LSP | – | – | – | – | ± | ± | – |
| | Определение DoS-атак | – | – | – | – | – | – | – |

* – На момент написания статьи была обнаружена критическая уязвимость, позволяющая через HP OpenView выполнить произвольный код на любом устройстве управляемой сети.

** – Мониторинг SLA поддерживается только при работе с оборудованием Cisco и Avaya.

Из проведенного анализа можно сделать заключение, что существующие системы управления ориентированы исключительно на сбор информации о сети и ее анализ. Управление сетью осуществляется непосредственно системным администратором, АСУ в данном случае выступает в роли «помощника», предлагая администратору выбрать один из предложенных вариантов решения проблемы. Некоторые АСУ содержат модули моделирования поведения ТКС, позволяющие оценить надежность сети, выявить «узкие места» и предоставить отчет о возможности реализации новых сервисов. Ни одна из рассмотренных систем не решает задачи управления отказами, динамической балансировки нагрузки или динамического распределения ресурсов. Эти задачи перекладываются на соответствующие протоколы, причем управление параметрами этих протоколов отсутствует. Поддержка MPLS ограничивается стандартным мониторингом с помощью SNMP и поддержкой MPLS VPN. Средства мониторинга и

управления LSP, как правило, отсутствуют. Также не реализованы алгоритмы выявления и борьбы с DoS-атаками.

Проведенный анализ показал, что разработка алгоритмов динамического управления ресурсами сети является актуальной.

Список литературы

1. Recommendation M.3010. Principles for a Telecommunications management network / ITU-T, 1996. – 81 p.
2. Recommendation M.3400. TMN Management Functions / ITU-T, 2000. – 110 p.
3. RFC 4377 Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks. The Internet Society, 2006 – 15p.
4. MPLS Fundamentals / Luc De Ghein. – Cisco Press, 2006. – 672 p.

Поступила в редколлегию 21.11.2011

Рецензент: д-р техн. наук, проф. Ю.И. Лосев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ МЕРЕЖАМИ MPLS

К.М. Руккас, К.А. Овчинников, Н.О. Королук

Наведено основні вимоги до систем управління мережею MPLS. Наведено огляд можливостей сучасних програмних продуктів різних виробників, що реалізують функції управління мережею MPLS із зазначенням особливостей архітектури, методів і протоколів збору та обробки статистично інформації, системних вимог і платформ, що підтримуються. Проведено порівняльний аналіз можливостей існуючих систем управління щодо вимог міжнародних стандартів ITU і IETF. Виявлено відсутність механізмів динамічного управління мережею і значна невідповідність вимогам, що висуваються до мереж MPLS.

Ключові слова: система управління мережею, мультипротокольна комутація по мітках, простий протокол управління мережами.

COMPARATIVE ANALYSIS OF MODERN CONTROL SYSTEMS FOR MPLS NETWORKS

K.M. Rukkas, K.A. Ovchinnikov, N.A. Koroljuk

The basic requirements for network management MPLS are set. An overview of modern software products from different manufacturers that implement MPLS network management functions is given. The features of the architecture, methods, and protocols for collecting and processing the statistical information, system requirements and supported platforms are marked. A comparative analysis of existing control systems based on the requirements of international standards ITU and IETF has been done. The absence of mechanisms of dynamic network management and a significant discrepancy referring to the requirements to networks MPLS were detected.

Keywords: network management system, Multi-Protocol Label Switching, a simple network management protocol.