Network Working Group
Request for Comments: 3410
Obsoletes: 2570
Category: Informational

J. Case
SNMP Research, Inc.
R. Mundy
Network Associates Laboratories
D. Partain
Ericsson
B. Stewart
Retired

December 2002

Введение и заявление о применимости модели стандартного управления Internet

Introduction and Applicability Statements for Internet Standard Management Framework

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задаёт каких-либо стандартов Internet. Распространение документа не ограничено.

Авторские права

Аннотация

Целью этого документа является обзор третьей версии модели стандартного управления Internet, называемой моделью SNMP[1] версии 3 (SNMPv3). Эта модель построена на основе исходного стандарта системы управления Internet (SNMPv1) и его второй версии (SNMPv2).

Модель использует модульную архитектуру, которая обеспечивает возможность её развития.

В этом документе приведено объяснение высокой целесообразности использования SNMPv3 взамен SNMPv1 и SNMPv2. Документ также служит рекомендацией к отказу от применения RFC 1157, 1441, 1901, 1909 и 1910 с переводом документов в статус Historic. Данный документ отменяет действие RFC 2570.

Оглавление

[1]Simple Network Management Protocol - простой протокол сетевого управления.

1. Введение

Этот документ служит введением для третьей версии стандарта управления Internet, названной SNMP версии 3 (SNMPv3) и имеет несколько целей.

Во-первых, описаны соотношения спецификации SNMPv3 со спецификациями SNMPv1, SNMPv2 и основанной на группах модели администрирования для SNMPv2.

Во-вторых, документ служит обзором множества спецификаций, относящихся к данной теме.

В-третьих, документ содержит краткие и понятные резюме для каждой из относящихся к теме спецификаций.

Этот документ осознанно написан, как учебный, и по этой причине иногда может казаться чересчур упрощённым. При возникновении противоречий между данным документом и более подробными спецификациями, для которых этот документ служит обзором, преимущество следует отдавать спецификации.

Кроме того, в подробных спецификациях предпринимаются попытки разделить компоненты системы для задания чётких интерфейсов между ними. В этом обзорном документе предпринимается попытка дать цельное представление всех модулей-компонент для лучшего понимания.

Документ является результатом работы группы SNMPv3 в рамках IETF[1].

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14, RFC 2119 [1].

2. Модель стандартного управления Internet

Третья версия модели стандартного управления Internet (модель SNMPv3) разработана на основе исходной спецификации SNMPv1 и второй версии SNMPv2.

Все версии (SNMPv1, SNMPv2, SNMPv3) модели стандартного управления Internet SNMP используют единую базовую структуру и компоненты. Более того, во всех версиях спецификации применяется общая архитектура.

2.1. Базовая структура и компоненты

Стандартная система управления в масштабе предприятия включает 4 основных компоненты:

- множество управляемых узлов, каждый из которых включает агент SNMP, обеспечивающий удалённый доступ с целью управления (agent);
- по крайней мере один объект SNMP с управляющими приложениями (его называют менеджером - manager);
- протокол управления для передачи управляющей информации между элементами SNMP;
- управляющая информация.

Протокол управления служит для обмена информацией между элементами SNMP (агентами и менеджерами).

Базовая структура совпадает для всех версия модели стандартного управления Internet (SNMPv1, SNMPv2, SNMPv3).

2.2. Архитектура модели стандартного управления Internet

Спецификации модели стандартного управления Internet основаны на модульной архитектуре. Модель является не просто протоколом обмена данными и включает:

- язык определения данных;
- определения управляющий информации (MIB[2]);
- определение протокола;
- защиту и администрирование.

С течением времени модель управления развивалась от SNMPv1 черезSNMPv2 до SNMPv3 и определения каждой из компонент архитектуры расширялись и прояснялись, но сама архитектура не менялась.

Одним из основных мотивов создания модульной архитектуры послужило стремление обеспечить возможность развития модели управления, как описано в RFC 1052 [2]. Изначальная идея заключалась в обеспечении возможности перехода от управления сетями на основе SNMP к управлению на базе протоколов OSI. По этой причине архитектура модели была основана на независимом от протоколов языке определения данных и MIB вместе с независимым от MIB протоколом. Такое разделение позволяет заменить основанный на SNMP протокол без переопределения и замены управляющей информации. Опыт показал, что выбор архитектуры был верным, несмотря на ошибочные мотивы. Этот выбор обеспечил простоту перехода от SNMPv1 к SNMPv2, а потом от SNMPv2 к SNMPv3, однако отказ от протокола SNMP оказался непосильной задачей.

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Management Information Base.

В модели SNMPv3 используются те же архитектурные принципы и добавлены расширения:

- построение на основе 4 базовых компонент архитектуры со встраиванием в некоторых случаев ссылок на SNMPv2;
- использование того же деления на уровни с определением новых возможностей в плане безопасности и администрирования.

Те, кто хорошо знаком с архитектурой управления SNMPv1 и SNMPv2, увидят множество знакомых концепций в архитектуре модели управления SNMPv3. Однако в ряде случаев может использоваться иная терминология.

3. Модель управления SNMPv1

Исходная модель стандартного управления Internet (SNMPv1) определена в нескольких документах:

- STD 16, RFC 1155 [3] определяет структуру управляющей информации (SMI[1]), а также механизмы описания и именования объектов в целях управления;
- STD 16, RFC 1212 [4] даёт более чёткие описания механизмов именования и описания информационных объектов управления, полностью согласованные с SMI;
- STD 15, RFC 1157 [5] определяет простой протокол управления сетями (SNMP), служащий для доступа через сеть к объектам управления и уведомлений о событиях. В этом документе определён также начальный набор уведомлений о событиях.

Обычно приведённый список дополняют ещё двумя документами:

- STD 17, RFC 1213 [6] содержит определения для базового набора управляющей информации;
- RFC 1215 [7] содержит чёткое описание механизма для определения уведомлений о событиях, которые в SNMPv1 обозначают термином trap (ловушка, прерывание). Документ также задаёт базовые прерывания из RFC 1157 в принятой нотации.

Эти документы описывают четыре части первой версии модели управления SNMP.

3.1. Язык управления данными SNMPv1

Первые два и последний документ (RFC 1155, 1212, 1215) описывают язык определения данных SNMPv1 и зачастую эти документы совместно обозначают термином SMIv1. Отметим, что в результате изначального требования независимости SMI от протоколов, первые два документа SMI не содержат способов определения уведомлений о событиях (trap). Взамен этого протокольный документ SNMP определяет несколько стандартизованных уведомлений о событиях (generic trap) о обеспечивает средства для определения дополнительных уведомлений о событиях. Последний документ определяет прямой подход для определения уведомлений о событиях, используемый протоколом SNMPv1. На момент написания указанного документа использование прерываний (trap) в схеме стандартного управления Internet не считалось бесспорным. По этой причине RFC 1215 со статусом Informational, не обновлялся впоследствии, поскольку предполагалось, что вторая версия модели SNMP заменит первую.

3.2. Данные управления

Язык определения данных, описанный в первых двух документах, впервые был использован для определения MIB-I, как указано в RFC 1066 [8], а впоследствии использовался для определения MIB-II, как указано в RFC 1213 [6].

Позднее, после публикации MIB-II, был изменён подход к определению управляющей информации, когда определение Internet-Standard MIB разрабатывалось единым комитетом в форме одного документа. Вместо этого стали создавать множество документов мини-MIB параллельно в разных рабочих группах, разрабатывающих спецификации для определённой части Internet-Standard MIB и включающих персонал с опытом в соответствующих областях (от различных аспектов управления сетью до управления системами и приложениями).

3.3. Работа протокола

Третий документ, STD 15 [5], описывает операции протокола SNMPv1, выполняемые протокольными модулями данных (PDU) над переменными, а также описывает формат сообщений SNMPv1. Для протокола SNMPv1 определены операции get (получить), get-next (получить следующую), get-response (получить отклик), set-request (запрос установки) и trap (прерывание). Определены также типовые уровни SNMP для транспорта без организации явных соединений.

3.4. Безопасность и администрирование SNMPv1

STD 15 [5] также описывает модели безопасности и администрирования. Многие из этих концепций были направлены в будущее, а некоторые, особенно в безопасности, были расширены в модели SNMPv3.

Модель SNMPv1 описывает инкапсуляцию SNMPv1 PDU в сообщения SNMP между элементами и обозначает различия между прикладными и протокольными элементами. В SNMPv3 их называют приложениями и устройствами (engine), соответственно.

В модели SNMPv1 введена концепция службы аутентификации, поддерживающей одну или несколько аутентификационных схем. В дополнение к аутентификации SNMPv3 определяет дополнительную опцию защиты, называемую конфиденциальностью (privacy)[2]. Модульная природа модели SNMPv3 позволяет как изменение, так и расширение возможностей защиты.

[1] Structure of Management Information.

[2] В части литературы, посвящённой безопасности, средства обеспечения безопасности SNMPv3 рассматриваются, как аутентификация источников, защита целостности и конфиденциальности.

Кроме того, в модели SNMPv1 введён контроль доступа на основе концепции представления SNMP MIB. В SNMPv3 дана спецификация фундаментально схожей концепции, названной контролем доступа на основе представления. С её помощью SNMPv3 обеспечивает контролируемый доступ к информации на управляемых устройствах.

Хотя модель SNMPv1 предполагает определение множества схем аутентификации, она не определяет никаких схем за исключением тривиальной аутентификации на основе строк community. Это является фундаментальным недостатком модели SNMPv1, но в то время определение защиты коммерческого класса могло представляться спорным с точки зрения устройства и сложным в реализации, поскольку меры защиты применялись очень разные. По этой причине и в результате отсутствия потребности в строгой аутентификации в архитектуре SNMPv1 службы аутентификации были вынесены в «отдельный блок» для последующего определения и модель SNMPv3 определяет архитектуру для использования в рамках этого блока и определения его подсистем.

4. Модель управления SNMPv2

Модель управления SNMPv2 описана в документах [8-13], а вопросы сосуществования и перехода от SNMPv1 к SNMPv2 рассмотрены в [15].

SNMPv2 обеспечивает ряд преимуществ по сравнению с SNMPv1, включая:

- расширенные типы данных (например, 64-битовые счётчики);
- повышение эффективности и производительности (оператор get-bulk);
- подтверждаемые уведомления о событиях (оператор inform);
- расширенную обработку ошибок (ошибки и исключительные ситуации);
- расширенные операции установки, особенно для создания и удаления строк;
- уточнения языка определения данных.

Однако описанная в этих документах модель SNMPv2 не полна в смысле соответствия исходным целям проекта SNMPv2. Не реализованы средства администрирования и обеспечения безопасности, обеспечивающие «коммерческий уровень» безопасности:

- аутентификация: идентификация источников, целостность сообщений и некоторые аспекты защиты от повторного использования сообщений;
- конфиденциальность;
- проверка полномочий и контроль доступа;
- подходящие возможности удалённой настройки и администрирования для перечисленных выше механизмов.

Описанная в этом и дополняющих его документах модель SNMPv3 решает эти важные вопросы.

5. Рабочая группа SNMPv3

Этот документ и дополнения к нему были подготовлены рабочей группой SNMPv3 IETF. Группа SNMPv3 была создана для подготовки рекомендаций по следующему поколению SNMP. Цель группы заключалась в создании требуемого набора документов для единого стандарта следующего поколения базовых функций SNMP. Одной из наиболее важных потребностей в разработке новых документов послужила необходимость определения механизмов защиты и администрирования, которые обеспечат безопасность управляющих транзакций SNMP и будут полезны для управления на базе SNMPv3 сетями, включёнными в них системами, а также работающими на этих системах приложениями, включая взаимодействия «менеджер-агент», «агент-менеджер» и «менеджер-менеджер».

За несколько лет до создания рабочей группы было предпринято много усилий, направленных на встраивание в SNMP защиты и других улучшений. Результатами этих работ стали:

- SNMP Security, 1991-1992 (RFC 1351 - RFC 1353),
- SMP, 1992-1993,
- The Party-based SNMPv2 (иногда называется SNMPv2p), 1993-1995 (RFC 1441 - RFC 1452).

Все эти разработки включали сильную защиту коммерческого уровня с поддержкой аутентификации, конфиденциальности, проверки полномочий, контроля доступа на основе представлений и администрирование, включающее удалённую настройку конфигурации.

Эти работы получили дальнейшее развитие в модели SNMPv2, описанной в RFC 1902 - 1908. Однако описанная в этих документах модель не включает стандартизованной модели защиты и администрирования и предлагает несколько вариантов решения таких задач, включая:

- SNMPv2 (SNMPv2c), RFC 1901 [16],
- SNMPv2u, RFC 1909 и 1910,
- SNMPv2*.

SNMPv2c получил наибольшую поддержку IETF, но не включает средств защиты и администрирования, тогда как SNMPv2u и SNMPv2* включают защиту, но не получили достаточной поддержки в IETF.

Рабочая группа SNMPv3 была создана для разработки единого комплекта спецификаций следующего поколения SNMP на основе сближения концепций и технических элементов SNMPv2u и SNMPv2*, как было предложено консультационной группой, которая была сформирована для разработки единого подхода к развитию SNMP.

Для выполнения поставленных задач рабочая группа определила следующие цели:

- приспособить модель к разным операционным средам с различными потребностями управления;
- продвигать необходимость перехода от множества предшествующих протоколов к SNMPv3;
- упростить работы по установке и обслуживанию.

На начальных этапах работы группа SNMPv3 сосредоточилась на вопросах защиты и администрирования, включая:

- аутентификацию и конфиденциальность;
- проверку полномочий и контроль доступа на основе представлений;
- стандартизованная удалённая настройка конфигурации перечисленного выше.

Группа SNMPv3 не занималась «изобретением велосипеда» и воспользовалась документами проектов стандартов SNMPv2 (т. е., RFC 1902 - 1908) в той части, которая выходила за упомянутую выше сферу сосредоточения.

Взамен основные участники SNMPv3 и группа в целом приложили существенные усилия к решению задач администрирования и защиты, значительно продвинув разработку современной модели сетевого управления.

Была разработана модульная архитектура с возможностью эволюционного развития по уровням. В результате SNMPv3 можно рассматривать, как SNMPv2 с дополнительными возможностями защиты и администрирования.

Сделав это, рабочая группа достигла цели создания единой спецификации, которая не только одобрена IETF, но и включает средства защиты и администрирования.

6. Спецификации SNMPv3

Спецификация SNMPv3 Management Framework разделена по модулям на несколько документов. Это осознанное решение рабочей группы SNMPv3 чтобы любой или все эти документы можно было пересматривать, обновлять или заменять по мере смены требований, обретения новых знаний и появления новых технологий.

Всякий раз, когда это возможно, исходный набор документов SNMPv3 Management Framework использует определения и реализации модели SNMPv2 с указанием ссылок на спецификации SNMPv2 Management Framework.

Модель SNMPv3 дополняет упомянутые спецификации в части администрирования и защиты для SNMPv3.

Документы, определяющие SNMPv3 Management Framework, используют такую же архитектуру, которая применялась предшественниками. Для удобства представления можно выделить несколько основных категорий:

- язык определения данных;
- модули (MIB);
- протокольные операции;
- безопасность и администрирование.

Документы из трёх первых категорий были взяты из SNMPv2. Документы четвертной категории являются новыми в SNMPv3, но, как отмечено выше, базируются в значительной мере на работах предшественников.

6.1. Язык определения данных

Спецификация языка определения данных включает STD 58, RFC 2578, Structure of Management Information Version 2 (SMIv2) [17] и связанные с ним документы. Эти документы обновляют RFC 1902 - 1904 [9-11], были разработаны независимо от других частей модели и опубликованы, как редакторские обновления в качестве STD 58, RFC 2578 - 2580 [17-19] в процессе продвижения от проекта (Draft Standard) к стандарту (Standard).

Структура управляющей информации SMIv2 определяет фундаментальные типы данных, модель объекта и правила написания и пересмотра модулей MIB. Связанные с ней спецификации включают STD 58, RFC 2579 и 2580.

STD 58, RFC 2579, "Textual Conventions for SMIv2" [18] определяет набор аббревиатур, доступных для использования во всех модулях MIB.

STD 58, RFC 2580, "Conformance Statements for SMIv2" [19] определяет формат заявлений о соответствии, используемых для описания требований к реализациям агентов, и заявлений о возможностях, используемых для документирования характеристик конкретных реализаций.

Термин SMIv2 является не вполне однозначным, поскольку используется по крайней мере в двух разных значениях. Иногда этим термином обозначают весь язык определения данных STD 58, описанный в RFC 2578 - 2580, а иногда - для обозначения лишь части языка определения данных, описанной в RFC 2578. Такая неоднозначность может причинять неудобства, но не вызывает существенных проблем.

6.2. Модули MIB

Модули MIB обычно содержат определения объектов, могут включать уведомления о событиях, а иногда содержат заявления о соответствии в терминах подходящих групп объектов и уведомлений о событиях. Таким образом, модули MIB определяют управляющую информацию, поддерживаемую в загружаемых узлах, делая её доступной для удалённых агентов управления. Эта информация передаётся с помощью протокола управления и обрабатывается управляющими приложениями.

Модули MIB определяются в соответствии с правилами, заданными в документах со спецификациями языка определения данных, прежде всего SMI.

Имеется и продолжает расти множество проектов стандартов с модулями MIB, указанных в периодически обновляемом документе Internet Official Protocol Standards [20]. На момент подготовки данного документа имелось более 100 модулей MIB, предложенных для стандартизации, с общим числом объектов более 10 000. Кроме того,

имеется и увеличивается множество фирменных модулей MIB, определяемых в одностороннем порядке производителями оборудования, исследовательскими группами, консорциумами, что приводит к возникновению не поддающегося учёту числа объектов.

В общем случае управляющая информация в любом модуле MIB (независимо от версии использованного языка определения данных) может применяться с любой версией протокола. Например, модули MIB, определённые в терминах SNMPv1 SMI (SMIv1), совместимы с моделью управления SNMPv3 Management Framework и могут переноситься с использованием описанных в ней протоколов. Более того, модули MIB, определённые в терминах SNMPv2 SMI (SMIv2), совместимы с протокольными операциями SNMPv1 и могут передаваться этим протоколом. Однако здесь имеется важное исключение - тип данных Counter64, который может присутствовать в модулях MIB формата SMIv2, не может передаваться протокольной машиной SNMPv1. Эти данные могут поддерживаться протоколами SNMPv2 и SNMPv3, но не будут переноситься машинами, поддерживающими только SNMPv1.

6.3. Протокольные операции и транспортные отображения

Спецификации для протокольных операций и транспортных отображений SNMPv3 задаются ссылками на документы SNMPv2, которые впоследствии были обновлены.

Спецификации протокольных операций заданы в STD 62, RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) [21].

Модель SNMPv3 разрабатывалась с учётом возможности независимого развития разных компонент архитектуры. Например, в этой модели может быть определена новая спецификация протокольных операций с целью расширения набора таких операций.

Спецификация транспортных отображений задана в STD 62, RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) [22].

6.4. Безопасность и администрирование SNMPv3

Серия документов, относящихся к защите и администрированию SNMPv3, которые были подготовлены рабочей группой SNMPv3 включает 7 RFC:

RFC 3410, Introduction and Applicability Statements for the Internet-Standard Management Framework - настоящий документ.

STD 62, RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [23] описывает архитектуру в целом, делая акцент на безопасности и администрировании.

STD 62, RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) [24] описывает возможность моделей множественной обработки сообщений и диспетчерскую часть протокольной машины SNMP.

STD 62, RFC 3413, Simple Network Management Protocol (SNMP) Applications [25] описывает 5 изначальных типов приложений, которые могут быть связаны с машиной SNMPv3 и её элементами.

STD 62, RFC 3414, User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3) [26] описывает угрозы, от которых обеспечивается защита, а также механизмы, протоколы и данные поддержки, используемые для защиты SNMP на уровне сообщений.

STD 62, RFC 3415, View-based Access Control Model (VCAM) for the Simple Network Management Protocol (SNMP) [27] описывает использование контроля доступа на основе представлений в приложениях для откликов на команды и уведомления инициаторов.

RFC 2576, SNMPv3 Coexistence and Transition [28] описывает сосуществование моделей управления SNMPv3, SNMPv2 и исходной SNMPv1. Документ находится в разработке.

7. Краткие описания документов

В последующих параграфах приводятся краткие описания перечисленных выше документов.

7.1. Структура управляющей информации

Управляющая информация рассматривается, как набор объектов управления, размещающихся в виртуальном хранилище информации, называемом базой MIB[1]. Наборы связанных объектов определяются в модулях MIB. Эти модули записываются с использованием языка определения данных SNMP, который создан на основе подмножества языка ASN.1[2] [29] OSI. Документы STD 58, RFC 2578, 2579, 2580 совместно определяют язык описания данных, задают базовые типы данных для объектов, базовый набор сокращённых обозначения типов данных для текстовых описания, а также некоторые административные привязки для значений идентификаторов объектов (OID).

SMI делится на три части - определения модулей, определения объектов и определения уведомлений.

(1) Определения модулей используются при описании информационных модулей. ASN.1-макрос MODULE-IDENTITY служит для краткой передачи семантики информационного модуля.

(2) Определения объектов используются для описания управляемых объектов. ASN.1-макрос OBJECT-TYPE служит для краткой передачи синтаксиса и семантики управляемого объекта.

(3) Определения уведомлений используются для описания незапрошенной передачи управляющей информации. ASN.1-макрос NOTIFICATION-TYPE служит для краткой передачи синтаксиса и семантики уведомления.

Как было отмечено выше, термин SMIv2 трактуется по разному и имеет, по крайней мере, два значения. Иногда этим термином обозначают язык определения данных STD 58 в целом, описанный в RFC 2578 - 2580, а иногда - только

[1]Management Information Base.
[2]Abstract Syntax Notation One.

часть языка определения данных, описанную в RFC 2578. Такая неоднозначность может причинять неудобства, но на практике редко приводит к серьёзным проблемам.

7.1.1. Базовая спецификация SMI
STD 58, RFC 2578 задаёт базовые типы данных для языка определения данных, которые включают: Integer32, перечисляемые целые числа (enumerated), Unsigned32, Gauge32, Counter32, Counter64, TimeTicks, INTEGER, OCTET STRING, OBJECT IDENTIFIER, IpAddress, Opaque, BITS. В документе также определены некоторые идентификаторы объектов. STD 58, RFC 2578 определяет перечисленные ниже конструкции языка определения данных.

- IMPORTS позволяет указать элементы, используемые в модуле MIB, но определённые в других модулях MIB;
- MODULE-IDENTITY позволяет указать для модуля MIB описание и административные данные (контакты, история версий и т. п.);
- OBJECT-IDENTITY и присваивание значений OID;
- OBJECT-TYPE для указания типа данных, статуса и семантики управляемых объектов;
- SEQUENCE для присвоения списка значений колонке таблицы;
- NOTIFICATION-TYPE для указания уведомлений о событиях.

7.1.2. Текстовые соглашения
При разработке модуля MIB часто бывает полезно указать (в краткой форме) семантику набора объектов с похожим поведением. Это делается путём определения нового типа данных, использующего базовый тип из спецификации SMI. Каждый новый тип имеет своё имя и указывает базовый тип с более ограниченной семантикой. Эти новые типы называют текстовыми соглашениями и они служат для удобства людей, читающих модуль MIB, а также «интеллектуальный» приложений сетевого управления. Целью документа STD 58, RFC 2579 Textual Conventions for SMIv2 [18] является определение конструкции TEXTUAL-CONVENTION языка определения данных, служащей для определения таких новых типов, и задание начального набора текстовых соглашений, доступного для всех модулей MIB.

7.1.3. Заявления о соответствии
Может оказаться полезным указание приемлемой нижней границы реализации вместе с реально обеспечиваемым уровнем. Целью STD 58, RFC 2580 Conformance Statements for SMIv2 [19] является определение конструкций языка определения данных, служащих для этого. Имеется два вида таких конструкций:

(1) Заявления о соответствии, используемые при описании требований к агентам в части определений объектов и уведомлений о событиях. Конструкция MODULE-COMPLIANCE служит для передачи сжатой формы таких требований.

(2) Заявление о возможностях служит для описания возможностей агентов в части определения объектов и уведомлений о событиях. Конструкция AGENT-CAPABILITIES служит для передачи такой информации в сжатой форме.

Наборы связанных объектов и уведомлений о событиях группируются в блоки соответствия. Конструкция OBJECT-GROUP служит включения объектов в группу и сжатой передачи информации о семантике группы. Конструкция NOTIFICATION-GROUP служит для включения уведомлений в группу и сжатой передачи информации о её семантике.

7.2. Работа протокола
Протокол управления служит для обмена сообщениями, которые переносят информацию между агентами и станциями управления. Сообщения имеют форму «обёртки», инкапсулирующей PDU[1].

Целью STD 62, RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) [21] является определение операций протокола, отвечающих за передачу и приём PDU.

7.3. Транспортные отображения
Сообщения SNMP могут применяться с разными стеками протоколов. Цель STD 62, RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP) [22] состоит в определении отображения сообщений SNMP на начальный набор транспорта. В будущем могут быть разработаны другие определения.

Определено несколько отображений, однако предпочтительным является отображение на транспортный протокол UDP. Поэтому для обеспечения максимального уровня совместимости системам, использующим иные отображения, следует также поддерживать посреднические услуги для отображений UDP.

7.4. Инструментарий
Целью STD 62, RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) [30] является определение управляемых объектов, описывающих поведение компонент элемента SNMP.

7.5. Архитектура - безопасность и администрирование
Целью STD 62, RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [23] является определение архитектуры для описания модели управления. Решая общие архитектурные вопросы, документ фокусируется на аспектах, связанных с администрированием и безопасностью. В документе определено множество терминов, применяемых в модели управленияSNMPv3, которые разъясняют и расширяют трактовки:

[1]Protocol Data Unit - модуль данных протокола.

- машин (engine) и приложений;
- элементов (поставщиков услуг типа машин в агентах и менеджерах);
- субъектов (пользователей услуг);
- управляющей информации, включая поддержку множества логических контекстов.

Документ включает небольшой модуль MIB, реализуемый всеми надёжными протокольными машинами SNMPv3.

7.6. Обработка и диспетчеризация сообщений (MPD)

STD 62, RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) [24] описывает обработку и диспетчеризацию сообщений в архитектуре SNMP. Документ определяет процедуры диспетчеризации сообщений разных версий SNMP в подходящие модели обработки сообщений SNMP, а также диспетчеризации PDU в приложения SNMP. Документ также описывает модель обработки сообщений (Message Processing Model) SNMPv3.

Машина протокола SNMPv3 **должна** поддерживать по крайней мере одну модель обработки сообщений. Протокольная машина SNMPv3 **может** поддерживать более одной модели (например, в системах, поддерживающих SNMPv3, SNMPv1 и/или SNMPv2c).

7.7. Применение SNMP

Целью STD 62, RFC 3413 Simple Network Management Protocol (SNMP) Applications [25] является описание пяти типов приложений, которые могут быть связаны с машиной SNMP. Эти типы включают генераторы команд (Command Generator), ответчики на команды (Command Responder), источники уведомлений (Notification Originator), получатели уведомлений (Notification Receiver), и пересылающие посредники (Proxy Forwarder).

Документ также определяет модули MIB для указания целей управляющих операций (включая уведомления), фильтрации уведомлений и пересылки.

7.8. Модель безопасности USM

STD 62, RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [26] описывает модель безопасности для SNMPv3. Документ определяет элементы процедуры (Elements of Procedure) для обеспечения защиты SNMP на уровне сообщений.

В документе рассмотрены две основные и две второстепенные угрозы, представляющие опасность для модели USM. К ним относятся изменение информации, маскировка, изменение потока сообщений и раскрытие информации.

USM использует MD5 [31] и SHA[1] [32] в качестве алгоритмов хэширования ключей [33] для расчёта цифровой подписи при защите целостности данных:

- прямая защита от атак с изменением данных;
- опосредованная аутентификация источника данных
- защита от атак с маскированием.

USM использует свободно синхронизируемые, монотонно возрастающие временные метки для защиты от атак с целью изменения потока сообщений. Заданы механизмы автоматической синхронизации часов на основе протокола без привлечения сторонних источников синхронизации и дополнительных требований безопасности.

USM использует алгоритм DES[2] [34] в режиме CBC[3], если нужна защита от раскрытия информации. Поддержка DES в модели USM является опциональной прежде всего по причине ограничений на экспорт и применение в ряде стран, осложняющих экспорт продукции, использующей криптографические технологии.

Документ включает также MIB, подходящую для удалённого мониторинга и управления конфигурационными параметрами для USM, включая распространение ключей и управление ими.

Элемент (объект) может одновременно поддерживать несколько моделей защиты, равно как и множество протоколов аутентификации и конфиденциальности. Все используемые USM протоколы основаны на применении заранее известных (т. е., секретных) ключей. Архитектура SNMPv3 позволяет использовать как симметричные, так и асимметричные (их часто называют криптографией с открытым ключом) механизмы и протоколы, но на момент написания этого документа не было моделей защиты SNMPv3 на базе открытых ключей для стандартизации IETF.

Продолжается работа по спецификации применения алгоритма AES в модели USM. Это будет отдельный документ.

7.9. Контроль доступа на основе представлений (VACM)

Целью STD 62, RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [27] является описание модели контроля доступа на основе представлений (VACM) в архитектуре SNMP. VACM в рамках одной реализации может быть связана с множеством моделей обработки сообщений и моделей безопасности.

Архитектура допускает наличие множества (разных) активных моделей контроля доступа в одной реализации, но предполагается, что на практике такие ситуации будут кране редкими и значительно менее распространёнными, нежели одновременное использование множества моделей обработки сообщений и моделей безопасности.

[1] Secure Hash Algorithm - алгоритм защитного хэширования.
[2] Data Encryption Standard - стандарт шифрования данных.
[3] Cipher block chaining - цепочка шифрованных блоков.

7.10. Сосуществование и переход к SNMPv3

Целью RFC 2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework [28] является описание сосуществования моделей управления SNMPv3, SNMPv2 и SNMPv1. В частности, документ описывает четыре аспекта сосуществования:

- преобразование документов MIB из формата SMIv1 в формат SMIv2;
- отображение параметров уведомлений;
- модели сосуществования элементов, поддерживающих разные версии SNMP в неоднородных в плане управления сетях и, в частности, выполнение протокольных операций в таких средах, а также поведение реализаций посредников;
- модель обработки сообщений SNMPv1 и модель безопасности, основанная на группах (Community-Based Security Model), обеспечивающие механизм адаптации SNMPv1 и SNMPv2c в модель VACM [27]

8. Статус стандартизации

Для выяснения текущего статуса стандартизации читателям рекомендуется обратиться к списку Internet Official Protocol Standards [20].

Однако рабочая группа SNMPv3 в тексте этого документа явно запрашивает повышения статуса SMIv1, SNMPv1 и SNMPv2c.

8.1. Статус SMIv1

SMIv1, как описано в STD 16 (RFC 1155 и 1212), был предложен в статусе Standard в 1990 и остаётся в этом статусе даже после того, как SMIv2 был предоставлен статус Standard (см. RFC 2026 [35], где приведена информация о процессах стандартизации Internet). Во многих случаях статус Standard меняется на Historic после того, как будет полностью стандартизована замена. Например, MIB-1 [8] был переведён в статус Historic после того, как MIB-2 [6] получил статус Standard. Аналогично, при достижении SMIv2 статуса Standard, было бы разумно отозвать статус SMIv1 и перевести его в категорию Historic, но в результате осознанного решения RFC 1155 и 1212 (STD 16) сохраняют статус Standard, но перестают быть рекомендуемыми. Эти документы не переведены в категорию устаревших (Historic) и остаются проектами стандартов, поскольку они указаны в качестве нормативных ссылок в других проектах стандартов и не могут быть переведены в категорию Historic без перевода в эту же категорию опирающихся на них документов. Следовательно, STD 16 сохраняет свой статус, но не рекомендуется по причине замены более новой спецификацией SMIv2.

На практике примерно с 1993 года для пользователей языка определения данных стало разумно применять SMIv2 во всех работах, поскольку реальные потребности в некоторых случаях диктуют необходимость поддержки форматов SMIv1 и SMIv2. В то время как уже есть недорогие и даже бесплатные инструменты для трансляции определений SMIv2 в определения SMIv1, создавать инструменты для автоматической трансляции определений SMIv1 в определения SMIv2 непрактично. Следовательно, для тех, кто работает в основном с SMIv2, предоставление данных также и в формате SMIv1 является тривиальной задачей. Напротив, те, кто работает с форматом SMIv1, сталкиваются со значительными издержками для обеспечения определений в обоих форматах - SMIv1 и SMIv2. Потребности современного рынка в определениях формата SMIv1 существенно снизились по сравнению с 1993 годом, а формат SMIv2 является значительно более предпочтительным, нежели SMIv1, хотя последний и не переведён в категорию устаревших. По этой причине IETF с настоящее время требует при написании новых модулей MIB пользоваться форматом SMIv2.

8.2. Статус стандартизации SNMPv1 и SNMPv2

Протокольные операции на основе сообщений SNMPv1 и SNMPv2c поддерживают только тривиальную аутентификацию на базе текстовых строк community (группа), что не обеспечивает должной защиты. Когда спецификация SNMPv3 в части защиты и администрирования получила статус Standard, стандартная (ранее, STD 15) спецификация SNMPv1 [5] и экспериментальная спецификация SNMPv2c, описанная в RFC 1901 [16], были объявлены устаревшими (Historic) по причине слабости защиты, а а взамен выбрана третья версия модели стандартного управления Internet. SNMPv2 (SNMPv2p), SNMPv2u и SNMPv2* были объявлены устаревшими в 1995 г или никогда не включались в процесс стандартизации.

На практическом уровне предполагается, что многие производители будут продолжать выпускать продукцию с поддержкой SNMPv1 и/или SNMPv2c, наряду с SNMPv3, а пользователи продолжат развёртывание и использование «многоязычных» реализаций. Следует отметить, что процесс стандартизации IETF не контролирует действия пользователей и производителей, которые могут продвигать развёртывать устаревшие протоколы типа SNMPv1 и SNMPv2c, несмотря на их недостатки. Однако не предполагается производство и развёртывание «многоязычных» реализаций с поддержкой SNMPv2p, SNMPv2u, SNMPv2*.

Действительно, как было отмечено выше, одна из спецификаций SNMPv3 в части защиты и администрирования - RFC 2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Management Framework [28], решает именно эти вопросы.

Конечно, важно, чтобы пользователи, разворачивающие многоязычные системы с незащищёнными протоколами проявляли осмотрительность и ограничивали доступ по протоколам SNMPv1 и SNMPv2c в соответствии с принятой в организации политикой безопасности. Точно также следует осмотрительно ограничивать доступ по протоколу SNMPv3 без аутентификации и защиты конфиденциальности, поскольку эти варианты близки с точки зрения безопасности. Например, во многих случаях неразумно будет предоставлять для SNMPv1 или SNMPv2c большие права доступа, нежели непроверенным пользователям SNMPv3 (нет смысла ставить вооружённую охрану и собак у парадной двери, если чёрный ход не охраняется совсем).

В моделях SNMPv1, SNMPv2 и SNMPv2c возможности администрирования протоколов SNMPv1 и SNMPv2c были весьма ограничены. Например, не было определений объектов для просмотра и настройки групп (community) или

получателей уведомлений (trap и inform). В результате производители сами определяли механизмы администрирования - от фирменных конфигурационных файлов, которые невозможно было просматривать и редактировать через SNMP, до специфичных для предприятия определений объектов. Модель SNMPv3 обеспечивает множество стандартизованных средств администрирования, которые могут применяться с протоколами SNMPv1 и SNMPv2c. Таким образом, для обеспечения должной совместимости при администрировании SNMPv1 и SNMPv2c в многоязычных системах следует использовать механизмы и объекты определённые в [25], [27] и [28] взамен соответствующих фирменных механизмов.

8.3. Рекомендации рабочей группы

В соответствии с приведёнными выше объяснениями рабочая группа SNMPv3 рекомендует перевести RFC 1157, 1441, 1901, 1909 и 1910 в статус Historical.

9. Вопросы безопасности

Поскольку этот документ, прежде всего, является обзором других документов, он не порождает новых вопросов, связанных с безопасностью. Читателю рекомендуется обратиться к соответствующим разделам рассмотренных здесь документов.

10. Литература

10.1. Нормативные документы

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March, 1997.

10.2. Дополнительная литература

[2] Cerf, V., "IAB Recommendations for the Development of Internet Network Management Standards", RFC 1052, April 1988.

[3] Rose, M. and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based internets", STD 16, RFC 1155, May 1990.

[4] Rose, M. and K. McCloghrie, "Concise MIB Definitions", STD 16, RFC 1212, March 1991.

[5] Case, J., Fedor, M., Schoffstall, M. and Davin, J., "Simple Network Management Protocol", STD 15, RFC 1157, May 1990.

[6] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", STD 17, RFC 1213, March 1991.

[7] Rose, M., "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991.

[8] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets", RFC 1156, March 1990.

[9] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1902, January 1996.

[10] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1903, January 1996.

[11] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1904, January 1996.

[12] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, January 1996.

[13] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1906, January 1996.

[14] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1907, January 1996.

[15] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Coexistence between Version 1 and Version 2 of the Internet-Standard Network Management Framework", RFC 2576, January 1996.

[16] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1901, January 1996.

[17] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[18] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[19] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[20] "Official Internet Protocol Standards", http://www.rfc-editor.org/rfcxx00.html, STD0001.

[21] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[22] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[23] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[24] Case, J., Harrington, D., Presuhn, R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[25] Levi, D., Meyer, P. and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[26] Blumenthal, U. and B. Wijnen, "User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[27] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[28] Frye, R., Levi, D., Routhier, S. and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework", RFC 2576, March 2000.

[29] Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), International Organization for Standardization. International Standard 8824, (December, 1987).

[30] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.

[31] Rivest, R., "Message Digest Algorithm MD5", RFC 1321, April 1992.

[32] Secure Hash Algorithm. NIST FIPS 180-1, (April, 1995) http://csrc.nist.gov/fips/fip180-1.txt (ASCII) http://csrc.nist.gov/fips/fip180-1.ps (Postscript)

[33] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[34] Data Encryption Standard, National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) Publication 46-1. Supersedes FIPS Publication 46, (January, 1977; reaffirmed January, 1988).

[35] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October, 1996.

11. Адреса редакторов

Jeffrey Case
SNMP Research, Inc.
3001 Kimberlin Heights Road
Knoxville, TN 37920-9716
USA
Phone: +1 865 573 1434
EMail: case@snmp.com

Russ Mundy
Network Associates Laboratories
15204 Omega Drive, Suite 300
Rockville, MD 20850-4601
USA
Phone: +1 301 947 7107
EMail: mundy@tislabs.com

David Partain
Ericsson
P.O. Box 1248
SE-581 12 Linkoping
Sweden
Phone: +46 13 28 41 44
EMail: David.Partain@ericsson.com

Bob Stewart
В отставке.

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

12. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.