**SNMP**

SNMP (англ. Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

При использовании SNMP один или более административных компьютеров (называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой системе есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт информацию менеджеру.

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

* Управляемое устройство;
* Агент — программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства;
* Система сетевого управления (Network Management System, NMS) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети

**Управляемое устройство** — элемент сети (оборудование или программное средство), реализующий интерфейс управления (не обязательно SNMP), который разрешает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютеры-хосты, принтеры и т. п.

**Агентом** называется программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства. Агент обладает локальным знанием управляющей информации и переводит эту информацию в специфичную для SNMP форму или из неё (медиация данных).

В состав **Системы сетевого управления (NMS)** входит приложение, отслеживающее и контролирующее управляемые устройства. NMS обеспечивают основную часть обработки данных, необходимых для сетевого управления. В любой управляемой сети может быть одна и более NMS.

**MIB**

Так как адреса объектов устройств определяются в цифровом формате, их сложно запомнить. Для упрощения применяются базы управляющей информации (MIB). Базы MIB описывают структуру управляемых данных на подсистеме устройства; они используют иерархическое пространство имён, содержащее идентификаторы объектов (OID-ы). Каждый OID состоит из двух частей: текстового имени и SNMP адреса в цифровом виде. Базы MIB являются необязательными и выполняют вспомогательную роль по переводу имени объекта из человеческого формата (словесного) в формат SNMP (цифровой).

SNMP работает на прикладном уровне TCP/IP (седьмой уровень модели OSI). Агент SNMP получает запросы по UDP-порту 161. Менеджер может посылать запросы с любого доступного порта источника на порт агента. Ответ агента будет отправлен назад на порт источника на менеджере. Менеджер получает уведомления (Traps и InformRequests) по порту 162. Агент может генерировать уведомления с любого доступного порта.

Ниже перечислены семь протокольных единиц обмена SNMP:

**GetRequest**

Запрос от менеджера к объекту для получения значения переменной или списка переменных. Получение значений указанной переменной должно быть выполнено агентом как Атомарная операция. Менеджеру будет возвращён Response (ответ) с текущими значениями.

**SetRequest**

Запрос от менеджера к объекту для изменения переменной или списка переменных. Связанные переменные указываются в теле запроса. Изменения всех указанных переменных должны быть выполнены агентом как атомарная операция. Менеджеру будет возвращён Response с (текущими) новыми значениями переменных.

**GetNextRequest**

Запрос от менеджера к объекту для обнаружения доступных переменных и их значений. Менеджеру будет возвращён Response со связанными переменными для переменной, которая является следующей в базе MIB в лексикографическом порядке. Обход всей базы MIB агента может быть произведён итерационным использованием GetNextRequest, начиная с OID 0. Строки таблицы могут быть прочтены, если указать в запросе OID-ы колонок в связанных переменных.

**GetBulkRequest**

Улучшенная версия GetNextRequest. Запрос от менеджера к объекту для многочисленных итераций GetNextRequest. Менеджеру будет возвращён Response с несколькими связанными переменными, обойдёнными начиная со связанной переменной (переменных) в запросе. Специфичные для PDU поля non-repeaters и max-repetitions используются для контроля за поведением ответа. GetBulkRequest был введён в SNMPv2.

**Response**

Возвращает связанные переменные и значения от агента менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest и InformRequest. Уведомления об ошибках обеспечиваются полями статуса ошибки и индекса ошибки. Эта единица используется как ответ и на Get-, и на Set-запросы, в SNMPv1 называется GetResponse.

**Trap**

Асинхронное уведомление от агента — менеджеру. Включает в себя текущее значение sysUpTime, OID, определяющий тип trap (ловушки), и необязательные связанные переменные. Адресация получателя для ловушек определяется с помощью переменных trap-конфигурации в базе MIB. Формат trap-сообщения был изменён в SNMPv2 и PDU переименовали в SNMPv2-Trap.

**InformRequest**

Асинхронное уведомление от менеджера менеджеру или от агента менеджеру. Уведомления от менеджера менеджеру были возможны уже в SNMPv1 (с помощью Trap), но SNMP обычно работает на протоколе UDP, в котором доставка сообщений не гарантирована, и не сообщается о потерянных пакетах. InformRequest исправляет это обратным отправлением подтверждения о получении. Получатель отвечает Response-ом, повторяющим всю информацию из InformRequest. Этот PDU был введён в SNMPv2.

Версия 3

Хотя SNMPv3 не приносит никаких изменений в протокол помимо добавления криптографической защиты, он является улучшением за счёт новых текстовых соглашений, концепций и терминологии.

Безопасность была большой проблемой SNMP с самого появления. Аутентификация в SNMP версий 1 и 2 сводилась не более чем к паролю (строке сообщества), который пересылался в открытом виде между менеджером и агентом.

В отличие от SNMPv1 и v2, в SNMPv3 каждое сообщение содержит параметры безопасности, которые закодированы как строка октетов. Значение этих параметров зависит от используемой модели безопасности.

SNMPv3 предоставляет важные особенности безопасности:

* Аутентификация — определение источника сообщения.
* Конфиденциальность — шифрование пакетов для защиты от перехвата.
* Целостность — предотвращение изменений сообщений в пути, включая дополнительный механизм защиты от повторной трансляции перехваченного пакета.

Безопасность

SNMP версий 1 и 2c подвержены перехвату пакетов со строками сообщений, так как они не используют шифрование.

Все версии SNMP подвержены атакам грубой силой и словарным перебором для угадывания строк сообщества, строк аутентификации, ключей аутентификации, строк шифрования или ключей шифрования, поскольку они не используют «рукопожатие» вида запрос-ответ.

Хотя SNMP работает с TCP и другими протоколами, обычно он используется с UDP, то есть без установки соединения и с уязвимостью для атак подменой IP. Для ограничения SNMP-доступа могут быть использованы списки доступа к устройству, но и механизмы защиты SNMPv3 способны успешно мешать атакам.

Обширные возможности в настройке SNMP многими поставщиками не используются в полную силу, отчасти из-за недостатка безопасности в версиях SNMP до SNMPv3, а также из-за того, что многие устройства просто не могут быть настроены с помощью изменений отдельного объекта базы MIB.