

# Технология SNMP

Костюкович А.Е.

# Технология SNMP

(Простой протокол управления сетью)

**В связи с ростом популярности Интернета технология, основанная на протоколе SNMP по факту стала основной.**

**Протокол SNMP был принят в конце 90-х годов и вскоре помимо применения в Интернете стал стандартом для управления сетями передачи данных и корпоративными сетями.**

**SNMP существенно проще, хотя и лишен ряда возможностей, которыми обладает CMIP.**

**Широкому распространению SNMP способствовали:**

- простота
- невысокая стоимость реализации.

**Однако обратной стороной этих достоинств, стали присущие SNMP недостатки:**

- слабая защита от несанкционированного доступа
- непригодность к работе с большими массивами данных, в крупномасштабных сетях
- и др.

**Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в MIB.**

**Простота SNMP во многом определяется простотой MIB SNMP, особенно их первых версий MIB I и MIB II.**

**Кроме того, сам протокол SNMP также весьма несложен.**

**SNMP — это протокол типа «запрос-ответ», то есть на каждый запрос от менеджера, агент должен передать ответ.**

# SNMP включает в себя всего несколько команд (сообщений):

1. Команда **Get-request** используется менеджером для получения от агента значения какого-либо объекта по его имени
2. Команда **GetNext-request** используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов

3. С помощью команды **Get-response** агент SNMP передает менеджеру ответ на команды Get-request или GetNext-request
4. Команда **Set** используется менеджером для изменения значения какого-либо объекта. С помощью команды Set происходит собственно управление устройством
5. Команда **Trap** используется агентом для сообщения менеджеру о возникновении особой ситуации.

- Версия **SNMP v.2** добавляет к этому набору команду **Get-Bulk**, которая позволяет менеджеру получить несколько значений переменных за один запрос.
- **Inform** - Позволяет одному менеджеру послать информацию типа "trap" другому менеджеру и запросить ответ.



**SNMP использует дейтаграммный транспортный протокол UDP, не обеспечивающий надежной доставки сообщений.**

**Сообщения SNMP, в отличие от сообщений многих других коммуникационных протоколов, не имеют заголовков с фиксированными полями.**

**В соответствии с нотацией ASN.1 сообщение SNMP состоит из произвольного количества полей, и каждое поле предваряется описателем его типа и размера.**

**Протокол SNMPv1 описан в RFC 1157.**

**Сообщение SNMP состоит из трех полей**



- **Version** - версия протокола,
- **Community** - идентификатор общности

Поле **community**, используется для ограничения доступа к управляемой системе.

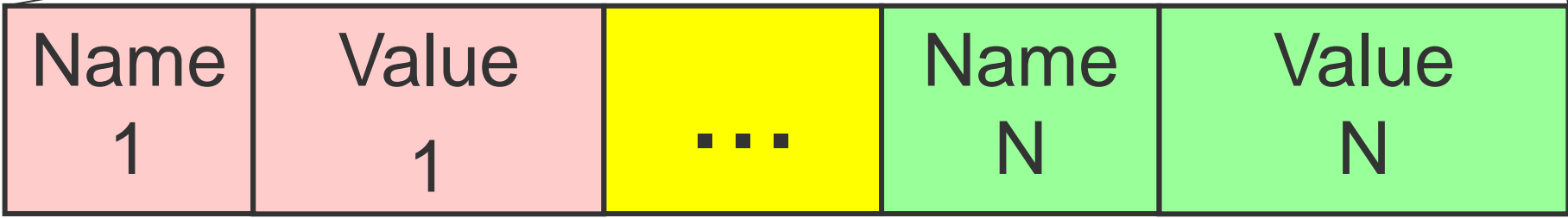
- **Блок данных (PDU)** – в данном поле определяется сущность запроса или ответа

**Блок данных (PDU) начинается с описания его типа (PDU type), который и определяет структуру блока.**

**В общем виде блок данных состоит из нескольких обязательных полей и произвольного числа имен (Name) и значений (Value) переменных.**

**Формат всех полей SNMP соответствует структуре **T-L-V (Tag-Length-Value)****

# Формат пакета PDU для Get, get-next, set и response имеет вид.



- **PDU type** – тип запроса-ответа (Get, Set,...)
- **Request-ID** - идентификатор (номер) запроса - Связывает запрос с ответом.
- **Error-status** - состояние сбоя - Сигнализирует о типе ошибки.
- **Error-index** - индекс ошибки - Связывает ошибку с частью переменных из поля "variable bindings".
- **Variable bindings** – переменные, связанные с данным запросом. В этом поле указываются **OID** запросов и ответов, а также значения запрашиваемых объектов

# Сравнение протоколов CMIP и SNMP

1. Агент SNMP выполняет самые простые функции и работает в основном по инициативе менеджера;
2. Система управления состоит из одного менеджера, который периодически опрашивает всех агентов;
3. SNMP опирается на простой, но не надежный транспортный протокол UDP;
4. Агент SNMP может послать данные менеджеру по своей инициативе с помощью сообщения trap.
5. Уведомление TRAP от агента посылается менеджеру без ожидания подтверждения, поэтому важные сетевые проблемы могут остаться незамеченными.
6. Протокол CMIP позволяет с помощью одной команды воздействовать на группу агентов, применив параметры ОБЗОР и ФИЛЬТРАЦИЯ
7. Агенты CMIP выполняют более сложные функции , чем агенты SNMP
8. CMIP рассчитан на интеллектуальных агентов, которые могут по одной простой команде от менеджера выполнить сложную последовательность действий.
9. Как следствие большей интеллектуальности агентов CMIP, трафик от протокола CMIP менее интенсивный чем от агентов SNMP.



**По мере развития сетей и технологии управления ими все более усложнялись версии SNMP.**

- Последняя версия SNMPv3 по функциональным возможностям приближается к протоколу CMIP, однако при этом теряется простота технологии SNMP**
- Последняя версия SNMP позволяет реализовать распределенную обработку, управляющей информации, т.е. часть функций по обработке может выполняться агентом.**
- Агенты SNMP становятся все более интеллектуальными, следовательно, более дорогими и рассчитаны на работу с последними версиями MIB-RMON**