

#### 44. Система управления на основе протокола SNMP

SNMP - это протокол прикладного уровня, разработанный для стека TCP/IP, хотя имеются его реализации и для других стеков, например IPX/SPX. Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base). В системах управления, построенных на базе SNMP стандартизируются: протокол взаимодействия агента и менеджера(SNMP), язык описания моделей MIB, модели MIB(MIB I,MIB II, RMON, RMON II), всё остальное отдано на ответственность разработчику.

SNMP - это протокол типа «запрос-ответ», то есть на каждый запрос, поступивший от менеджера, агент должен передать ответ. Особенностью протокола является его чрезвычайная простота - он включает в себя всего несколько команд.

- Команда Get-request используется менеджером для получения от агента значения какого-либо объекта по его имени.
- Команда GetNext-request используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов.
- С помощью команды Get-response агент SNMP передает менеджеру ответ на команды Get-request или GetNext-request.
- Команда Set используется менеджером для изменения значения какого-либо объекта. С помощью команды Set происходит собственно управление устройством.
- Команда Trap используется агентом для сообщения менеджеру о возникновении особой ситуации.
- Версия SNMP v.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько значений переменных за один запрос.

Структура SNMP MIB. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB

Версия MIB-I определяет 114 объектов, которые подразделяются на 8 групп.

- *System* - общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).
- *Interfaces* - параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).
- *Address Translation Table* - описание соответствия между сетевыми и физическими адресами (например, по протоколу ARP).
- *Internet Protocol* - данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика о IP-пакетах).
- *ICMP* - данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.
- *TCP* - данные, относящиеся к протоколу TCP (например, о TCP-соединениях)
- *UDP* - данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UDP-дейтаграмм).
- *EGP* - данные, относящиеся к протоколу обмена маршрутной информацией Exterior Gateway Protocol, используемому в Internet (число принятых с ошибками и без ошибок сообщений).

В версии MIB-II был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10.

*Спецификация RMON MIB.* Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами

Объект RMON объединяет 10 групп следующих объектов.

- *Statistics* - текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т. п.
- *History* - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
- *Alarms* - пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру.
- *Hosts* - данные о хостах сети, в том числе и о их MAC - адресах.
- *HostTopN* - таблица наиболее загруженных хостов сети.

- Traffic Matrix - статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы.
- Filter - условия фильтрации пакетов.
- Packet Capture - условия захвата пакетов.
- Event - условия регистрации и генерации событий.

Всего стандарт RMON MIB определяет около 200 объектов в 10 группах. Отличительной чертой стандарта RMON MIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому он удобен для гетерогенных сред, использующих различные протоколы сетевого уровня.

Недостатки протокола SNMP:

- нет средств взаимной аутентификации агентов и менеджеров
- работа по протоколу UDP, который не обеспечивает надежную доставку сообщений