Федеральное агентство по образованию

Нижневартовский государственный гуманитарный университет

Факультет информационных технологий и математики

Кафедра информатики и методики преподавания информатики

КОНТРОЛЬНАЯ РАБОТА

Администрирование в информационных системах

Вариант №1

Выполнил: студент 4 курса

42 группы ИСиТ

Сабиров Р.З.

Проверил

**Петров Д. А.**

Нижневартовск – 2012

**ПРОТОКОЛ SNMP.** [**RFC 3411**](http://tools.ietf.org/html/rfc3411)**.**

*SNMP (англ. Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определен Инженерным советом интернета (IETF) как компонент TCP/IP. Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.*

*SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы. Эти переменные могут быть запрошены (а иногда и заданы) управляющими приложениями.*

**Обзор и основные понятия.**

При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые *менеджерами*) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. С каждой управляемой системой связана постоянно запущенная программа, называемая *агент*, которая через SNMP передаёт информацию менеджеру.

*Агенты* SNMP обрабатывают данные о конфигурации и функционировании управляемых систем и преобразуют их во внутренний формат, удобный для поддержания протокола SNMP. Протокол также разрешает активные задачи управления, например, изменение и применение новой конфигурации через удаленное изменение этих переменных. Доступные через SNMP переменные организованы в иерархии. Эти иерархии, как и другие метаданные (например, тип и описание переменной), описываются базами управляющей информации (базы MIB, от англ. *Management information base*).

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. Управляющие 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.

В силу своего названия - *Простой Протокол Сетевого Управления* - основной задачей при его разработке было добиться максимальной простоты его реализации.

В результате возник *протокол, включающий минимальный набор команд, однако позволяющий выполнять практически весь спектр задач управления сетевыми устройствами* - от получения информации о местонахождении конкретного устройства, до возможности производить его тестирование.

Основной концепцией протокола является то, что вся необходимая для управления устройством информация хранится на самом устройстве - будь то сервер, модем или маршрутизатор - в так называемой **Административной Базе Данных** (MIB - *Management Information Base*).

**MIB** представляет из себя *набор переменных, характеризующих состояние объекта управления*. Эти переменные могут отражать такие параметры, как количество пакетов, обработанных устройством, состояние его интерфейсов, время функционирования устройства и т.п.

Каждый производитель сетевого оборудования, помимо стандартных переменных, включает в MIB какие-либо параметры, специфичные для данного устройства. Однако, при этом не нарушается принцип представления и доступа к административной информации - все они будут переменными в MIB.

Поэтому SNMP как непосредственно сетевой протокол предоставляет только набор команд для работы с переменными MIB. Этот набор включает следующие операции:

|  |  |
| --- | --- |
| get-request | Используется для запроса одного или более параметров MIB |
| get-next-request | Используется для последовательного чтения значений. Обычно используется для чтения значений из таблиц. После запроса первой строки при помощи get-request get-next-request используют для чтения оставшихся строк таблицы |
| set-request | Используется для установки значения одной или более переменных MIB |
| get-response | Возвращает ответ на запрос get-request, get-next-request или set-request |
| trap | Уведомительное сообщение о событиях типа cold или warm restart или "падении" некоторого link'а. |
|  |  |

Для того, чтобы проконтролировать работу некоторого устройства сети, необходимо просто получить доступ к его MIB, которая постоянно обновляется самим устройством, и проанализировать значения некоторых переменных.

Важной особенностью протокола SNMP является то, что в нем *не содержатся конкретные команды управления устройством*. Вместо определения всего возможного спектра таких команд, безусловно загромоздившего бы сам протокол, который считается все-таки простым, *определены переменные* MIB*, переключение которых воспринимается устройством как указание выполнить некоторую команду*.

Таким образом удается сохранить простоту протокола, но вместе с этим сделать его довольно мощным средством, дающим возможность стандартным образом задавать наборы команд управления сетевыми устройствами. Задача обеспечения выполнения команд состоит, таким образом, в регистрации специальных переменных MIB и реакции устройства на их изменения.

**ПРОТОКОЛ LDAP.**

Служба каталога (**Directory Service**) - *это программный комплекс для хранения и каталогизации информации*. По своей сути это очень *похоже на обычную базу данных*, но с «уклоном» скорее на чтение данных, нежели на их добавление или изменение. Обычно служба каталога базируется на клиент-серверной архитектуре. Одна из наиболее известных таких систем - DNS (**Domain Name Service**): DNS-сервер производит взаимную «трансляцию» имён машин и их IP-адресов. Другие машины в сети могут обращаться к такому серверу за информацией о соответствии имени и адреса. Однако это очень простой пример каталогизации информации. Объекты в такой базе имеют ограниченное количество атрибутов - таких как имя, адрес и ещё несколько дополнительных параметров. Разумеется, служба каталога какого-либо предприятия будет содержать более разнообразные данные и иметь гораздо более сложную структуру.

В общем случае, служба каталога должна предоставлять простой, централизованный доступ к данным, которые могут использоваться различными приложениями. Протокол, по которому могла бы работать такая служба, был разработан в ISO (**International Standartization Organization**), получил номер **X.500** и назывался DAP (**Directory Access Protocol**). В соответствии с этим протоколом любое приложение может получить доступ к информации в каталоге. Там же была предложена гибкая и легко расширяемая информационная структура, которая позволяла хранить, в принципе, любой тип данных. К сожалению, X.500 имел и ряд ограничений, среди которых зависимость от коммуникационного уровня, который не являлся стандартным протоколом TCP, и запутанность требований к правилам именования объектов. В результате решение на базе этого протокола становилось очень дорогим при обслуживании.

Позже появился протокол **LDAP** (**Lightweight Directory Access Protocol**), который *позволил реализовать доступ по TCP/IP и мог легко расширяться*. В результате появилось решение, позволяющее организовать службу каталога на предприятии любого масштаба.

Сегодня существует несколько реализаций данного протокола от различных фирм. Наиболее известные из них — Netscape Directory Service™, Novell Directory Service™ и Microsoft Active Directory™. Из некоммерческих реализаций LDAP наибольшее распространение получил проект **OpenLDAP**. Именно его мы и будем рассматривать в дальнейшем, хотя большинство понятий и определений применимо и к другим реализациям сервера LDAP.

**Основные термины**

Для понимания работы службы каталога необходимо усвоить несколько ключевых терминов.

* Данные каталога хранятся в виде объектов или сущностей (от англ. **entry**), состоящих из специальных полей, называемых **атрибутами** (**attributes**). Набор атрибутов, их синтаксис и правила поиска определяются **схемой каталога** (**scheme**). Все объекты каталога идентифицируются специальным атрибутом — DN (**Distinguished Name**).
* Данные в каталоге можно представить в виде древовидной структуры — DIT (**Directory Information Tree**). Это очень похоже на структуру, используемую многими файловыми системами. Вершиной такого дерева является **корневой объект** (**Root Entry**). DNкорневого объекта одновременно является **суффиксом каталога**.
* Каждый последующий объект в структуре каталога идентифицируется уникальным значением DN, который описывает путь к объекту в каталоге. Если продолжить аналогию с файловой системой, то DN любого объекта так же включает DN всех объектов стоящих выше по иерархии. Отличие в данном случае только в том, что DN формируется не слева направо, как путь к файлу, а наоборот — справа налево.
* **DN администратора каталога** (**Root Distinguished Name**) — это специальный объект, описывающий администратора каталога. Этот объект указывается в конфигурации сервера, но может отсутствовать в самом каталоге. К такому объекту не применяются списки доступа (**ACL**). В некоторых реализациях LDAP такой объект может не иметь суффикса.
* **База поиска** (**Base Distinguished Name**) — объект каталога, начиная с которого производится поиск. Дело в том, что не всегда есть необходимость производить поиск по всему дереву каталога; ограничить область поиска можно указанием в запросе базы поиска. По умолчанию этот параметр соответствует суффиксу.

**ПРОТОКОЛЫ POP3, IMAP, SMTP**

Без протоколов SMTP, РОРЗ и IMAP невозможна работа электронной почты. Надеюсь, что такое электронная почта и как без нее плохо, объяснять не нужно.

Особенностью этих протоколов является их узкая направленность. Это означает, что их принципиально невозможно использовать для других целей, что, к тому же, не имеет смысла. Задача SMTP, РОРЗ и IMAP — организация обмена электронными сообщениями, и они отлично с ней справляются.

Еще одной особенностью почтовых протоколов является однозадачность. Например, протокол, отсылающий сообщения, не способен их принимать, и наоборот. Именно поэтому такие протоколы работают парами.

**SMTP** (Simple Mail Transfer Protocol, упрощенный протокол пересылки почты) — протокол, основной задачей которого является отсылка подготовленных специальным образом сообщений. Перед тем, как это сделать, протокол устанавливает соединение между компьютерами, что гарантирует доставку сообщения.

Протокол SMTP очень простой и эффективный, однако эта эффективность не распространяется на все задачи и возможности. Так, он не обладает даже простейшим механизмом аутентификации и возможностью шифрования данных при передаче между почтовыми серверами. Самым большим недостатком SMTP является его неспособность к пересылке графики.

Чтобы не отказываться от этого довольно хорошего протокола, было принято решение расширить его несколькими полезными и необходимыми расширениями. Таким расширением, например, является MIME (Multipurpose Internet Mail Extensions, многоцелевое расширение почтовой службы в Интернете), благодаря которому существует возможность отсылать файлы любого формата и содержания. Кроме того, разработан стандарт UUENCODE, позволяющий передавать текстовые сообщения в разных кодировках.

**РОРЗ** (Post Office Protocol 3, почтовый протокол версии 3) — почтовый протокол, который используется для приема электронных сообщений с почтового сервера.

Обычно РОРЗ работает в паре с протоколом SMTP, что позволяет организовать эффективную систему отсылки и приема электронных сообщений.

Интерфейс протокола еще более простой, чем интерфейс SMTP, и с этим связаны определенные неудобства. Так, отсутствует возможность выборочного скачивания письма или просмотра содержимого письма непосредственно на почтовом сервере.

**IMAP** (англ. Internet Message Access Protocol) — протокол прикладного уровня для доступа к электронной почте.

Базируется на транспортном протоколе TCP и использует порт 143.

IMAP предоставляет пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

Для отправки писем используется протокол SMTP.