Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет» (НИУ)
Высшая школа электроники и компьютерных наук
Кафедра «Инфокоммуникационные технологии»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой ИКТ
_____ С.Н. Даровских
«____»_____2020 г.

Система мониторинга цифровой сети оператора связи на основе протокола SNMP

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ - Д 11.03.02.2020.237.00 ПЗ

Руководитель работы,
_____ В.В. Новиков
«____» _____2020 г.

Автор работы,
студент группы КЭ-411
_____ И.И. Хасанов
«____» _____2020 г.

Нормоконтролер,
_____ В.Д. Спицына
«____» _____2020 г.

Челябинск 2020

РЕФЕРАТ

Хасанов И.И. Система мониторинга цифровой сети оператора связи на основе протокола SNMP. – Челябинск: ЮУрГУ, ВШЭКН; 2020, 43 с., 4 табл., 24 ил., библиогр. список – 12 наим., 1 лист приложений, 2 плаката формата А1.

В данной выпускной квалификационной работе был рассмотрен протокол мониторинга и управления SNMP.

Цель работы заключается в том, чтобы создать тестовую среду, на котором можно применить инструменты управления и мониторинга, которым располагает SNMP.

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ASN.1 (Abstract Syntax Notation One) — в области телекоммуникаций и компьютерных сетей язык для описания абстрактного синтаксиса данных.

DTLS (Datagram Transport Layer Security) обеспечивает защищённость соединений для протоколов, использующих датаграммы.

IP (Internet Protocol) — маршрутизируемый протокол сетевого уровня стека TCP/IP.

ISO (The Open Systems Interconnection model) — сетевая модель стека сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом.

MIB (Management Information Base) база управляющей информации - виртуальная база данных, используемая для управления объектами в сети связи.

NMS (Network Management System) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети.

OID (Object Identifier) - это дополнительный и необязательный атрибут сертификата электронной подписи, который либо предоставляет дополнительную информацию о владельце, ключах, удостоверяющем центре, либо несёт какую-то дополнительную информацию для приложений и сервисов, которые используют этот сертификат электронной подписи.

PDU (Protocol Data Unit) — обобщённое название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент.

RFC (Request for Comment) — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети.

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

TCP – (Transmission Control Protocol — протокол управления передачей) — один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных.

UDP (User Datagram Protocol — протокол пользовательских датаграмм) — один из ключевых элементов набора сетевых протоколов для Интернета.

VLAN (Virtual Local Area Network) — топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований

ВВЕДЕНИЕ

Для благополучного управления и мониторинга в ip сетях с большим количеством сетевых устройств нужно знать статус каждого ее элемента и при необходимости изменить настройки. В большинстве случаев сеть обладала устройствами от разных производителей и возникали большие трудности в управление, так как у устройств были разные языки команд.

Следовательно появилась востребованность в разработке общего простого протокола для управления устройствами. У которого был бы общий язык для администрирования всех сетевых устройств.

В 1991 году разрабатывается SNMP (Simple Network Management Protocol). Со временем набирает популярность и становится стандартом для производителей сетевых оборудований. В основу протокола

В итоге появляется протокол, содержащий в себе минимум набор команд, но позволяющий реализовывать самые разнообразные задачи для управления и мониторинга.

1 Теоретическая часть

1.1 История развития протокола SNMP

В 1980 году резким событием стал тот факт, что в области топологии сетей начал происходить ощутимый рост. Что заставило прийти к новому решению, потому что проблемы связанные с увеличением сетей приводили многие организации в кризис. Компании расширяли существующие сети, тем самым, росла нагрузка на управление работой сети, а это требовало дополнительного набора персонала и ежедневного мониторинга. Нужен был простой инструмент, позволяющий управлять сетевыми устройствами[3].

В апреле 1988 после очередного заседания IAB(Internet Architecture Board) выпустили рабочее предложение, в котором требовалось сделать Простое Сетевое Управление.

Создание SNMP сразу вошла в обороты. И первая версия вышла в свет в мае 1991 года под документами(RFC 1155, RFC 1212, RFC 1213, RFC 1157). Для производителей сетевых оборудований эти документы дали толчок для внедрения данного протокола в свои оборудования. В наше время SNMP является самым популярным протоколом, встроен во все сетевые ОС(операционная система).

1.2 Обзор и основные понятия

Simple Network Management Protocol в переводе на русский – простой протокол сетевого управления. Представляет собой интернет-протокол позволяющий управлять и отслеживать за сетевыми устройствами, таких как роутеры, коммутаторы, серверы, принтеры и другими. На основе TCP/UDP. По модели OSI принадлежит уровню прикладной, которая поддерживает, к примеру, HTTP, FTP, POP3, WebSocket. Если устройство поддерживает SNMP, то этот протокол может собирать информацию о ней и сохранять в базе данных.

SNMP характеризуют три компонента:

- менеджер, запущенный на пользовательском хосте;

– агент, запущенный на сетевом устройстве;

– база данных MIB.

На рисунке 1 показано, как взаимодействуют три компонента между собой.

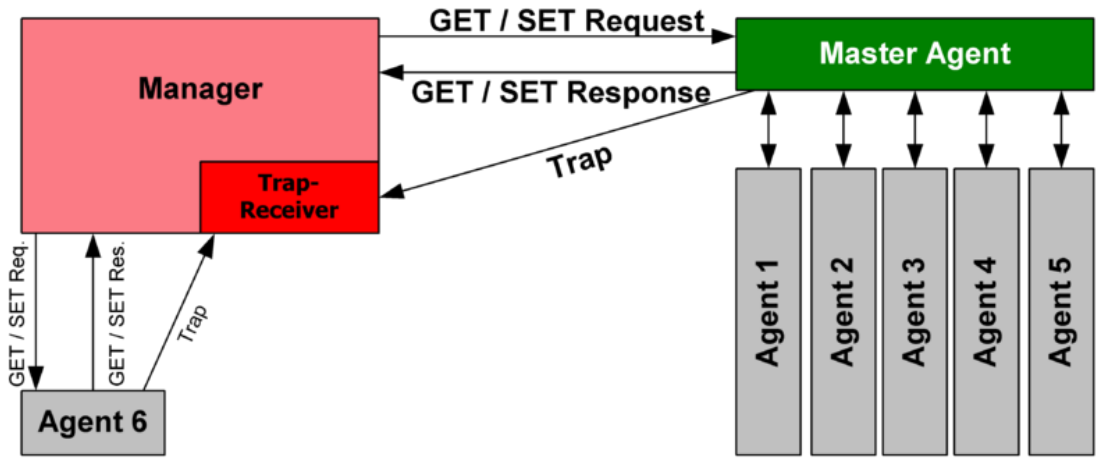


Рисунок 1- SNMP компоненты.

Управляемое устройство — элемент сети, реализующий интерфейс управления, который разрешает однонаправленный или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: роутеры, серверные оборудования, 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[1].

1.3 База управляющей информацией MIB

Каждый компьютер сети имеющий на своем порту SNMP агента он предоставляет свой некий набор данных, которое спроектировали разработчики. В любом сетевом устройстве, где поддерживается протокол SNMP существует иерархическая база MIB с обозначенным набором переменных и база имеет древовидную форму, каждый объект описывается неповторимым идентификатором объекта. Ветка MIB оканчивается переменной хранящий в себе определенные значения, которое сохраняется в переменную SNMP агента работающий на компьютере. Значения переменной описывает конкретный хост. Содержит в себе информацию о загрузки системы, состояние интерфейса и многое другое. Существует единое стандартизированное структурное дерево MIB. Существует всемирное дерево регистрации ISO – оно содержит базовую структуру миб. Дерево объектов MIB напоминает систему DNS, тоже есть свои символьные имена и соответствующие числовые значения. OID находится в библиотеке MIB. OID состоит из конкретных значений. Все это сделано для того, чтобы было легко запомнить и удобно работать[4].

Расположение стандартной ветки system, где содержатся такие, например, настройки как описание системы (sysDescr) и время прошедшее с запуска системы (sysUpTime) - 1.3.6.1.2.1.1. Расположение к параметру sysDescr - 1.3.6.1.2.1.1.1, прибавилась ещё 1, так как это первый параметр ветки. Расположение sysUpTime - 1.3.6.1.2.1.1.3 - третий параметр. На рисунке 2 изображена стандартная ветка от MIB.

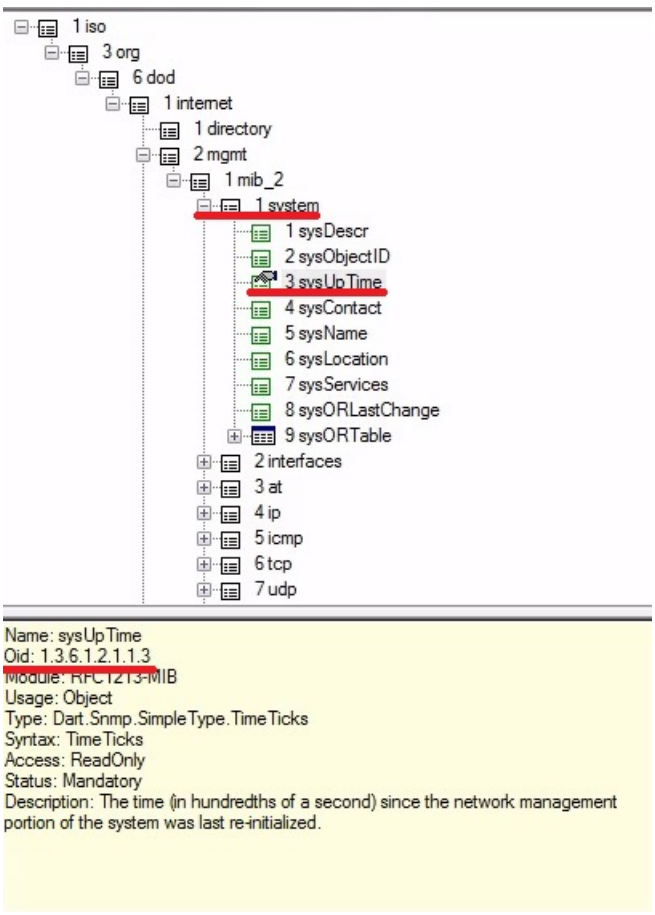


Рисунок 2 – структура OID

Проприетарные ветки производителей всегда располагаются по строго заданному пути iso.org.dod.internet.private.enterprises или в цифровом выражении 1.3.6.1.4.1.

1.4 Детали протокола

SNMP базируется на уровни стека протоколов TCP/IP – в модели OSI существует на седьмом уровне. Agent SNMP получает запросы по UDP-порта 161. Менеджер отправляет 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. При использовании

TLS или DTLS запросы получаются по порту 10161, а ловушки отправляются на порт 10162 [1].

В SNMPv1 указано пять основных протокольных единиц обмена (protocol data units — PDU). Еще две PDU, GetBulkRequest и InformRequest, были введены в SNMPv2 и перенесены в SNMPv3.

Все PDU протокола SNMP построены по рисунку 3.

IP header (IP-заголовок)	UDP header (UDP-заголовок)	version (версия)	community (пароль)	PDU-type (PDU-тип)	request-id (id запроса)	error-status (статус ошибки)	error-index (индекс ошибки)	variable bindings (связанные переменные)

Рисунок 3 – PDU

1.4.1 GetRequest

Запрос от менеджера к объекту для принятия значения переменной или списка переменных. Необходимые переменные вводятся в поле variable bindings Получение значений указанной переменной должно быть выполнено агентом как Атомарная операция. Менеджеру будет возвращён ответ с текущими значениями.

1.4.2 SetRequest

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

1.4.3 GetNextRequest

Запрос от менеджера к объекту для поиска доступных переменных и их значений. Менеджеру будет возвращён Response со связанными переменными для переменной, которая является следующей в базе MIB в лексикографическом порядке. Поиск 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.

1.4.3 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.

1.4.4 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 .

1.4.5 Trap

SNMP агент может не только опрашивать, но и само устройство может отправить уведомление с опережением. За это отвечают трапы. В этом есть

необходимость, когда нужно обнаружить разнообразные проблемы в сети. Например, упал порт или отключили питание. И в случае, если произойдет действие нарушающие привычную работу, то трап сообщит нам об этом.

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 [1].

1.4.6 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.

1.5 Разработка и использование

Всего на данный момент существуют 3 версии протокола SNMP. Это SNMPv1, основная задача которого просто опросить устройство. Без возможности авторизации. Далее разрабатывается версия SNMPv2c, включает авторизацию и производит опрос от заданного имени. Последний версией является SNMPv3 включающий в себя функции второго, но умеющий шифровать пароли и данные.

1.5.1 Версия SNMPv1

Самой изначальной разработкой протокола стала версия SNMv1. UDP, CLNS, IP взаимодействуют с данным протоколом. Версия 1 используется масштабно, но не является официальным стандартом(используется де-факто) и

предназначен для сетевого управления в прикладном уровне.

Версия 1 обладает низкой безопасностью. Поэтому по сей день, его практически не используют. Проверка и принятие информации выполняется благодаря community string(общей строки), то есть пароля, которая содержится в открытом виде. Разработчикам удалось за короткое время предложить промежуточный вариант протокола, в нем функционировал ограниченный набор инструментов(простой вопрос от OID и ответ на на него) и без возможности авторизации, не смотря на это, он был одобрен .

1.5.2 Версия SNMPv2c

После выпуска первой версии, многие понимали что у v1 много несовершенств, но чувствовался большой потенциал данного протокола и его необходимость. Поэтому практически сразу за v1 выходит v2, которая обладает похожими функциями из 1 версии, но с разными улучшениями. Протокол обрел более лучшую производительность, а безопасность, вовсе, выросла с нулевой отметки на пару пунктов. В протокол добавились такие команды как GetBulkRequest для управления.

1.5.3 Взаимодействие SNMPv1 и SNMPv2c

На данный период времени эти версии между собой несовместимы. Они используют различные форматы сообщений и операций протокола. Например, SNMPv2c включает в себя 2 операции протокола, а в SNMPv1 вовсе они отсутствуют. Однако, существует двуязычные ССУ и прокси-агенты на этом уровни две эти версии могут работать.

SNMPv2 может работать через прокси-агент от имени управляемых протоколом SNMPv1:

- система сетевого управления (Network management system, NMS) SNMPv2 сообщает строки, для SNMPv1-агента;
- NMS отправляет SNMP-сообщение прокси-агенту SNMPv2;

- прокси-агент без изменения направляет сообщения Get, GetNext и Set агенту SNMPv1;
- сообщения GetBulk преобразуются прокси-агентом в сообщения GetNext, после чего направляются агенту SNMPv1;
- прокси-агент отображает trap-сообщения SNMPv1 в trap-сообщения SNMPv2, после чего направляет их NMS[1].

Двуязычные SNMPv2-системы сетевого управления поддерживают как SNMPv1, так и SNMPv2. Для поддержки такого окружения управляющее приложение в двуязычной NMS должно связаться с агентом. Затем NMS анализирует хранящуюся в локальной базе данных информацию для определения, поддерживает ли агент SNMPv1 или SNMPv2. На основе этой информации NMS связывается с агентом, используя соответствующую версию SNMP.

1.5.4 Версия SNMPv3

Самая последняя версия считается безопасным для использования, но довольно трудной при настройке. Изменения, которые вошли в этот уровень, а именно внедрение криптографической защиты оцениваются как незначительные. Однако, текстовые документы соглашений, концепций и терминологий добавляют значительный плюс перед предыдущими версиями.

Значительно улучшилась защита. В самой первой разработке она отсутствовала вовсе. Во второй вся защита сводилась к паролю доступа в открытом в виде, который могли перехватить посторонние лица.

В новой версии все сообщения могут быть закодированы как строки октетов. В какие именно определялось от самой модели безопасности, которых было 3.

SNMPv3 существующие виды 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.

1.6 Как читать OID файлы

В таблице 1 приведены стандартные мибы, которые подходят для всех устройств. OID (1.3.6.1.2.1.1.5) означает, что в последовательности открываются вкладки, которые расположены в виде дерева и в конце под номером 5 попадает на sysName, в нем находиться информация об имени устройства. Для каждого объекта существует свой уникальный идентификатор, сделано это для того, чтобы удобно было работать с системой. В таблице 1 приведена стандартная ветка OID.

Таблица 1 - стандартная ветка OID

№	Название объекта	Расшифровка аббревиатур
1	iso	Internation Organization for Standardization (ISO)
3	Identifiled-organization	Схема определения организации согласно ISO/IEC 6523-2
6	dod	United States Department of Defense(DoD). Организация, которая изначально занималась стандартизацией протокола
1	internet	Интернет
2	mgmt	IETF Managment
1	mib-2	База OID для спецификации MIB-2
1	system	Характеристики системы
5	sysName	Имя системы

1.7 Технология VLAN

Эта главная функция коммутаторов. VLAN помогает объединить компьютеры в одну сеть на канальном уровне (второй уровень модель OSI). Даже

если они физически подключены к разным коммутаторам. Так же позволяет полностью изолировать траффик группы узлов от остальной сети. Отлично подходит для возможности выделения в отдельную сеть отдела организации или группы хостов используя общий коммутатор. VLAN основа построения любой сети, которая имеет несколько информационных ресурсов, строя логическую структуру сети. Ее удобно анализировать, чем обычную физическую схема, где изображены только подключения. При этом на высоком уровне обеспечивает безопасность, к примеру, разделяя сеть гостевых пользователей от сети серверов это значительно повысить безопасность, так как злоумышленник не получит доступ с гостевых хостов к серверам. Пользователи существующие на разных сегментах, могут взаимодействовать только на сетевом уровне(3 уровень модели OSI), а для этого уже необходим роутер или коммутатор L3 [9].

Преимущества:

- структурирует сеть;
- обеспечивает безопасность;
- объединения пользователей;
- широковещательный трафик.

1.8 Модель OSI

Одна из эталонных моделей организацией сетей, которая описывает из каких уровней должна состоять сеть и что должен делать тот или иной уровень. ISO(Модель взаимодействия открытых систем). Это юридический документ, который принят в качестве стандарта Международной организацией по стандартизации в 1983 году. Модель OSI состоит из 7 уровней и эта модель описывает назначение каждого из них. Не является сетевой архитектурой, так как не включает описание протоколов. Уровни моделей расположены друг над другом. Нумерация начинается снизу вверх(см. рисунок 4).

Модель OSI				
Уровень (layer)		Тип данных (PDU[11])	Функции	Примеры
Host layers	7. Прикладной (application)	Данные	Доступ к сетевым службам	HTTP, FTP, POP3, WebSocket
	6. Представления (*presentation*)		Представление и шифрование данных	ASCII, EBCDIC
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP, L2TP
	4. Транспортный (transport)	Сегменты (segment) / Дейтаграммы (datagram)	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, PORTS
Media[2] layers	3. Сетевой (network)	Пакеты (packet)	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk
	2. Канальный (data link)	Биты (bit)/ Кадры (frame)	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта.
	1. Физический (physical)	Биты (bit)	Работа со средой передачи, сигналами и двоичными данными	USB, кабель («витая пара», коаксиальный, оптоволоконный), радиоканал

Рисунок 4 – 7 уровней модели OSI

Физический уровень предназначен для передачи битов по каналу связи. Данный уровень не анализирует передаваемую информацию. Основная задача 1 уровня – это определить способ представления битов информации в виде сигналов, которые будут передаваться по среде передачи данных.

Канальный уровень, который находится над физическим. Он умеет в потоке бит выделять отдельные сообщения, которые приходят от физического уровня. Проверяются и исправляются ошибки передачи. И присваивается дополнительная служебная информация. Например, адрес отправителя и получателя.

Сетевой уровень нужен для построения крупных сетей на основе различных сетевых технологий. Обеспечивается согласование различий в разных технологиях канального уровня, предоставляется общая адресация с помощью глобальных адресов, которые помогают однозначно определить компьютеры в составной сети в независимости от технологии канального уровня. Выполняется маршрутизация.

Транспортный уровень обеспечивает передачу данных между процессами, которые находятся на разных компьютерах. Особенностью является, то что он может гарантировать более высокую надежность.

Сеансовый уровень создает сеансы связи для определения очередностей передачи сообщений в задачи управления диалогом. Например, видеоконференция в котором участвуют несколько человек и если все люди начнут говорить одновременно, то они нечего не услышат. Сеансовый уровень определяет, кто когда будет говорить, что бы все друг друга услышали. Решает задачи одновременного доступа к некоторым критическим операциям.

Уровень представления его задача предоставлять данные в таком виде, которое понятно как отправителя, так и получателю. Согласует формат данных и смысл. Например, разные хосты могут использовать различные кодировки для представления символов, или разные форматы хранения чисел.

Прикладной уровень – это набор приложений которые могут использовать пользователи сети. Это веб-страницы, скайп, социальные сети и многое другое. В таблице 2 указаны на каких уровнях существуют устройства.

Таблица 2 – Сетевое оборудование

Уровень модели OSI	Оборудование
Сетевой	Маршрутизатор
Канальный	Коммутатор, точка доступа
Физический	Концентратор

1.9 Модель и стек протоколов TCP/IP

TCP/IP первое, чем отличается от ISO, тем что она не является юридическим стандартом, а считается стандартом де-факто, который стал настолько популярным, что в итоге все стали его использовать. TCP/IP создавался для глобальных сетей чтобы объединить большие компьютеры, которые стояли в университетах по телефонным линиям связи. Когда появились новые технологии сетей такие как, ethernet, спутниковые адаптировать их под TCP/IP оказалось совсем не просто. Стало понятно, что нужна модель, которая будет говорить о

том, как люди должны строить сети на основе разных технологий. Модель TCP/IP включает 4 уровня:

- сетевой интерфейс – взаимодействие с различными сетевыми технологиями(ethernet и wi-fi);
- интернет – обеспечивает поиск маршрута в составной сети;
- транспортный – связь между двумя процессами;
- прикладной – набор приложений для пользователей.

Во многом TCP/IP и OSI схожи, у второго лучше проработаны теоритические аспекты в виде RFC документов, что позволяет упрощать настройки. Достоинством первого является, что оно широко используется на практике в сети интернет, но плохо пригоден для описания сетей.

1.9.1 Протокол UDP

В транспортном уровне на стеке протоколов TCP/IP существуют два протокола:

- TCP;
- UDP.

Надежная доставка данных обеспечена только на TCP, а в UDP ставка сделана исключительно на скорость доставки сообщения(дейтаграммы). На данном уровне нужно указывать порт отправителя и получателя. В таблице 3 указаны размеры заголовков в битах.

Таблица 3 – Формат заголовка UDP

16 бит – Порт отправителя	16 бит – Порт получателя
16 бит – Длина UDP	16 бит– Контрольная сумма UDP

Протокол UDP обеспечивает более высокую скорость работы благодаря тому, что не устанавливает связь между получателем и отправителем. Это

практически всегда оправдывается в современных сетях, так как ошибки возникают редко, и они могут быть исправлены на уровне приложения. Область применения в котором системы работают по принципу «запрос-ответ».

2 Практическая часть

2.1 Локальная сеть

Чтобы SNMP протокол воплотить на практике, нужна тестовая среда. Лучше всего управлять и мониторить локальной сетью построенной на программном симуляторе. Для получения практических навыков отлично подойдет Packer Tracer от компании Cisco. Для начала определим конфигурацию сети. Для реализация поставленных задач достаточно и простой сети, которая изображена на рисунке 5. В сеть будут включены:

- три хоста;
- один коммутатор;
- один маршрутизатор;
- коммутационные кабели.

Такими малыми составляющими обычно располагают малые офисы, где сотрудников работающих за компьютером не больше 10 человек[10].

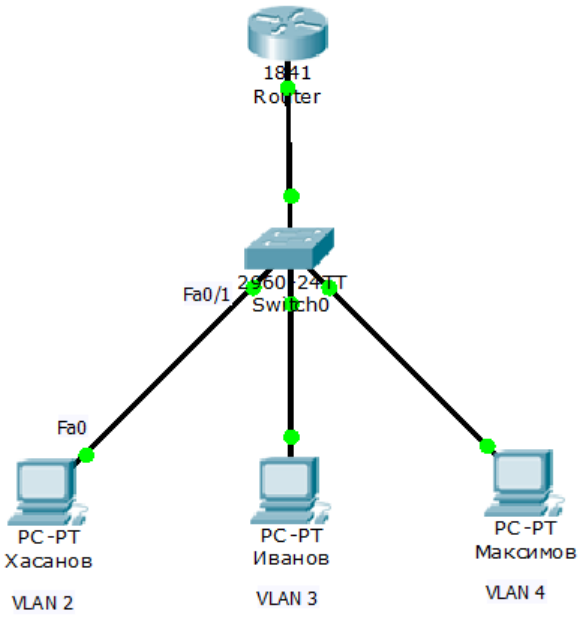


Рисунок 5 – простая сеть

На рисунке 3 наблюдается очень маленький внутренний трафик. Поэтому ставить L3 коммутатор, как минимум не рентабельно, они стоят в порядке 5000 тысяч долларов. Будет достаточно применение недорого маршрутизатора, который с легкостью способен организовать доступ для этих пользователей в интернет. В нашем случае будет выступать маршрутизатор cisco 1841.

Технические особенности cisco 1841:

- аппаратное ускорение шифрования для стандартов шифрования DES, 3DES, AES;
- WAN-интерфейс ISDN S/T BRI;
- USB порт и поддержка POE;
- встроенный сетевой адаптер;
- реализован 802.1Q VLAN;
- flash: 32-128 Mb, DRAM 128-384 Mb.

Для начала проведем нужные настройки коммутатора, который работает на втором уровне модели OSI, создадаем 3 сегмента, для этого нужно воспользоваться технологией VLAN. Откроем консоль Switch’a и создадим VLAN 2,3,4. После этого определим компьютеры в нужные сегменты, например, по рисунку 3, видно, что ПК Хасанов подключен к интерфейсу fa0/1. Благодаря, команде swithchport acces vlan 2, который изображен на рисунке 6, присуждается хост Хасанов к VLAN 2. Производим те же настройки с остальными хостами, только принадлежать они будут к другим вланам.

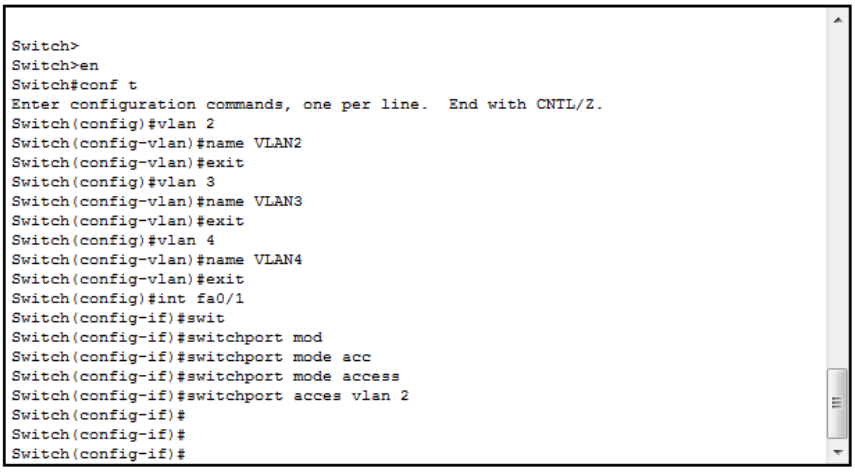


Рисунок 6 – настройка коммутатора

Теперь пользователи находятся на разных сегментах, и чтобы они могли взаимодействовать между собой нужно настроить специализированное маршрутизирующее устройство. Настраиваться будет уже знакомый cisco 1941. Переходим CLI, для начала включаем физический порт(fastEthernet 0/0), так как, у роутеров по умолчанию порты отключены. Порт поднимается командой no shotdown. На роутер приходят 3 VLAN’a, поэтому для них нужны подинтерфейсы.

Компьютеры так же нуждаются в прописывание ip адресов, масок и других конфигураций. В таблице 4 указаны их значения.

Таблица 4 - IP Configuration хостов

Имя пользователя	IP address	Subnet Mask	Default Gateway	Vlan
Хасанов	192.168.2.2	255.255.255.0	192.168.2.1	2
Иванов	192.168.3.2	255.255.255.0	192.168.3.1	3
Максимов	192.168.4.2	255.255.255.0	192.168.4.1	4

Настройка локальной сети на этом закончена. Проверяем с помощью команды ping работоспособность сети. Для этого с хоста Иванов(192.168.3.2) наберем ping Максимов(192.168.4.2) и определяем, есть ли связь. Как видно на рисунке 7, все работает.

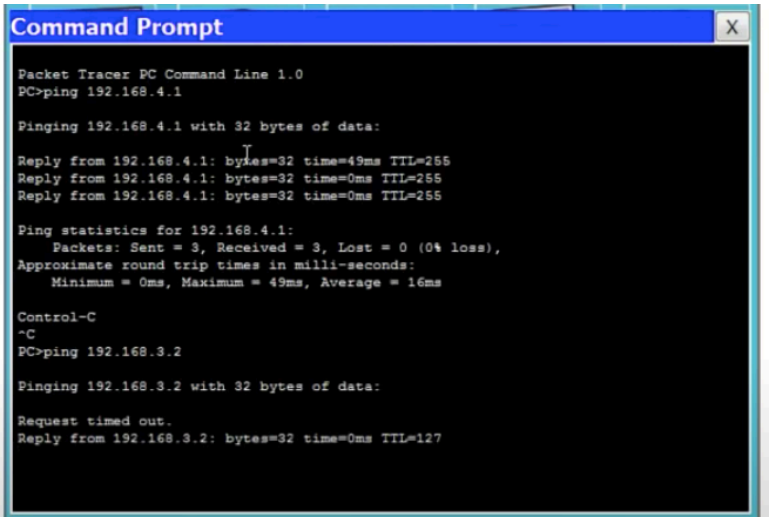


Рисунок 7 – обмен пакетами

Таким образом, с помощью маршрутизатора организовали маршрутизацию трафика между тремя сегментами.

2.2 MIB файлы

После того как построена локальная сеть, стоит посмотреть структуру базы данных данной сети, которая имеет древовидную форму. Она показана на рисунке 8.

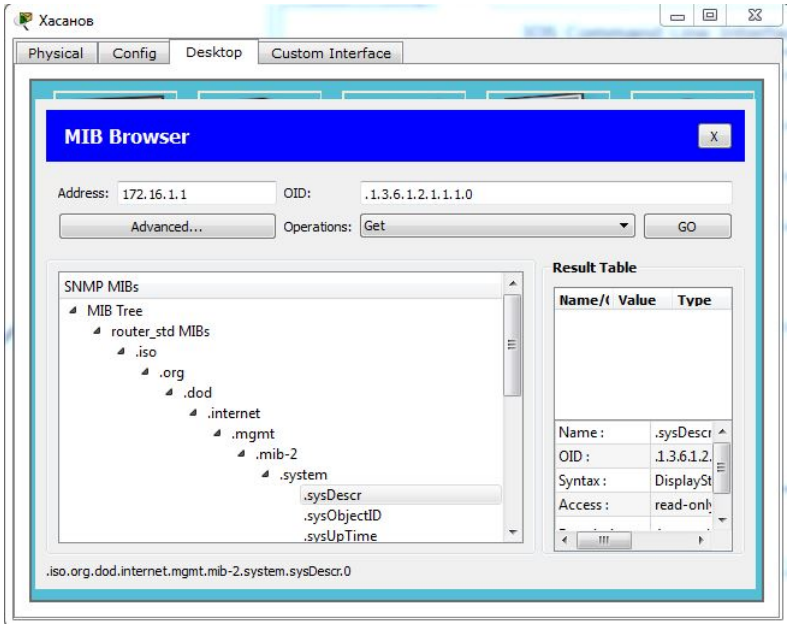


Рисунок 8 – структура MIB

Как правильно читать OID написано в пункте 1.6. Для демонстрации мониторинга и управления сетью поставим перед собой 2 задачи:

– определить продолжительность работы сети(мониторинг);

– изменить название роутера(управление).

Для этого воспользуемся 2 командами:

– Get (просмотр дерева OID-ов);

– Set (изменяет настройки).

Переходим в MIB Browser, в поле OID вводим числовое значение принадлежащие .sysUpTime, а именно .1.3.6.1.2.1.1.3.0. И набираем команду Get. Исходя из рисунка 9, наша сеть работает 2 часа 5 минут и 25 секунд.

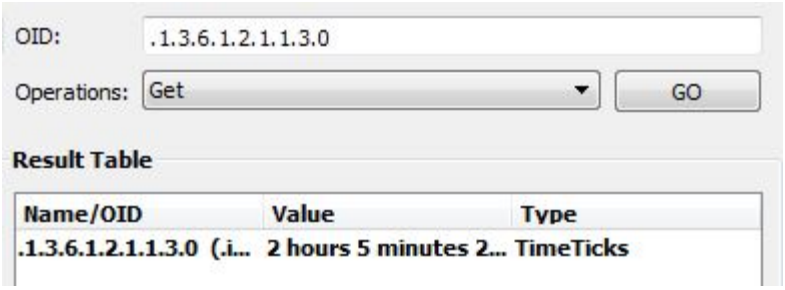


Рисунок 9 – время работы устройства

Далее вводим в OID .1.3.6.1.2.1.1.5.0, в поле Value новое название маршрутизатора. После команды Set изменения вступят в силу. По рисунку 10 видно, что в консоле изменилось имя с router2 на snmp.

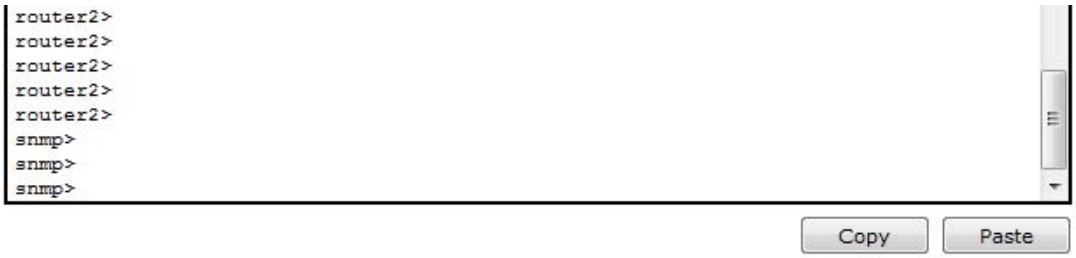


Рисунок 10 – название роутера

В результате осуществили простой мониторинг и управление сети на протоколе SNMP. Собрали всю необходимую информацию о функционирование сети в базу данных MIB и успешно поработали с ней.

2.3 Traps

Впоследствии использования протокола SNMP стало проявляться его другая необходимость. Где не пользователь опрашивает устройство, а где само устройство уведомляет нас с опережением, так называемые, трапы.

SNMP стал универсальным благодаря тому, что устройство может отправить текущее событие без нашего ведома. Например, отключили электроэнергию и мгновенно сработает функция последнего «мяу». И устройство

самостоятельно без нашего опроса отправит trap о событие. Чтобы не опрашивать устройство каждые несколько секунд, проще запросить протокол SNMP, и устройство будет сообщать обо всех подобных событиях.

Для реализации trap воспользуемся не cisco packet tracer(симулятор), а GNS3 – это программа эмулятор, максимально моделируют реальную среду. Интерфейс облака приведен на рисунке 11, в последующем он будет подключен к маршрутизатору c3725(см. рисунок 12).

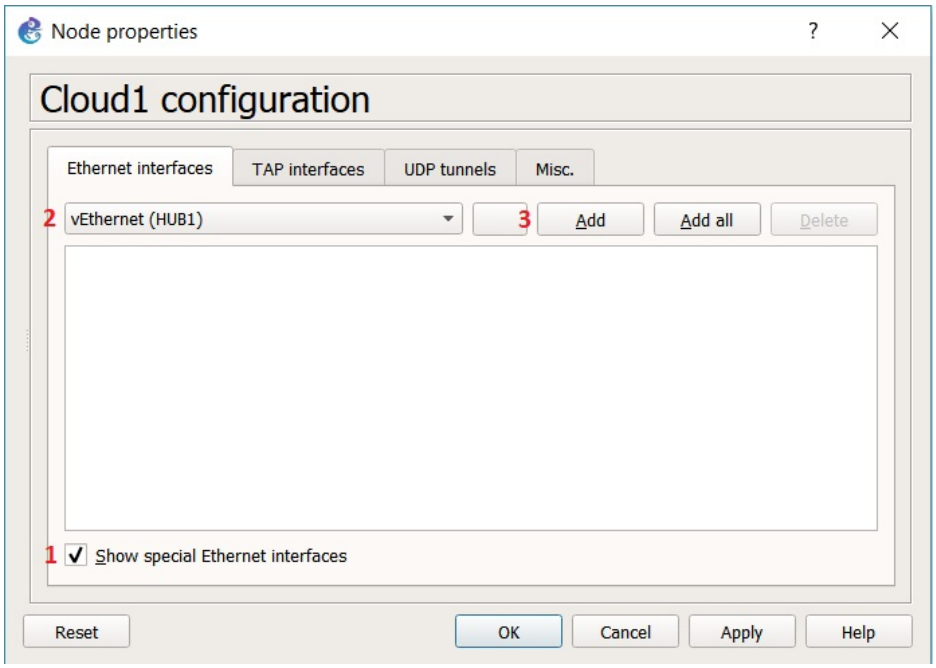


Рисунок 11 – интерфейс облака

Настройки:

- IP fa0/0 cisco - 192.168.136.2/24;
- IP ПК – 192.168.136.40/24;
- IP HUB1 – 192.168.136.1/24.

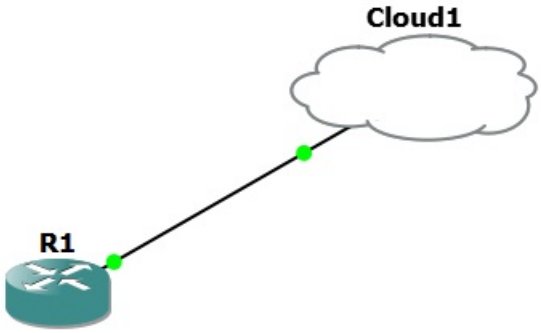


Рисунок 12 – cisco c3725 и облако

В версиях SNMP 1 и SNMP 2 производятся анологичные настройки.

В CISCO c3725 настроен только fastEthernet 0/0, который идет к облаку. В консоле ведем команду sh snmp g. По рисунку 13 видно, что создалось две группы на чтение Тест 1 и Тест 2.

```
R1(config)#snmp-server community TEST ro SNMP_ACL
R1(config)#end
R1#s
*Mar  1 00:03:31.047: %SYS-5-CONFIG_I: Configured from console by console
R1#sh snmp g
groupname: ILMI                           security model:v1
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                           security model:v2c
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: TEST                           security model:v1
readview : v1default                      writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: SNMP_ACL

groupname: TEST                           security model:v2c
readview : v1default                      writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: SNMP_ACL

R1#
```

Рисунок 13 – созданные группы

После чего удаляем сообщество и группы, рисунок 14. Далее создается сообщество с правом на запись по рисунку 15.

```
R1(config)# no snmp-server community TEST
ro SNMP_ACL
R1(config)# no snmp-server group TEST v1
R1(config)# no snmp-server group TEST v2
```

Рисунок 14 – TEST v1 и TEST v2

И создаем сообщество с правом на запись.

```
R1(config)# snmp-server community TEST rw
SNMP_ACL
```

Рисунок 15 – сообщество с правом на запись

На рисунке 16 красным отмечены 2 группы для версий 1 и 2 с правом на запись и чтение.

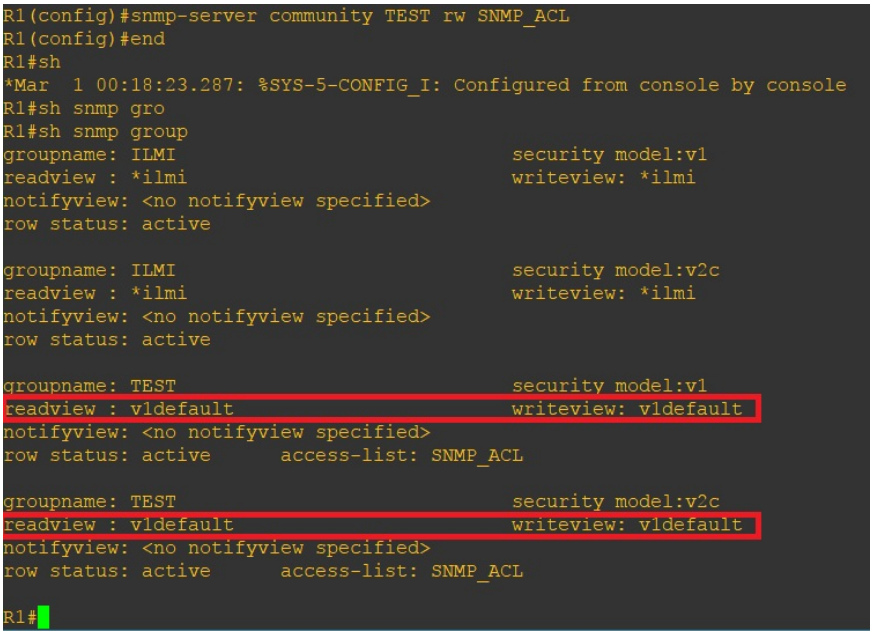


Рисунок 16 – консоль

В последующем в диспетчере для дальнейшей работы можно выбрать две версии на выбор.

Далее настройка роутера по рисунку 17.

```
R1(config)# ip access-list standard
SNMP_ACL
R1(config-std-nacl)#permit host
192.168.137.40
R1(config-std-nacl)#exit
R1(config)# snmp-server community TEST ro
SNMP_ACL
R1(config)# snmp-server host 192.168.137.40
version 1 TEST - или version 2c TEST
R1(config)# snmp-server enable traps snmp
```

Рисунок 17 – настройка маршрутизатора

Пояснения к командам изображенным на рисунке 17:

- строка 1 - SNMP_ACL(включает списки доступов);
- строка 2 – настройка списков доступа;
- строка 3 – выход из состояния config-std-nacl;
- строка 4 – создается agent snmp;
- строка 5 – в случае возникновение трапов, будет отсылать на 192.168.137.40;
- строка 6 – включить трапы(ловушки).

Типы ловушек входящие в snmp:

- authentication;
- linkdown;
- linkup;
- coldstart;

– warmstart.

Далее запускаем программу PowerSNMP Free Manager, который служит в роли диспетчера. После поиска доступных агентов в программе, в рисунке 18 видно их отсутствие и сработает трап authentication. Потому что поиск изначально запрещен доступом public, изменяем значения на ранее созданный TEST, впоследствии агент благополучно добавляется. Вводим интервал обновления и триггер, прописываем e-mail адрес, в случае ловушки агент отправит письмо.

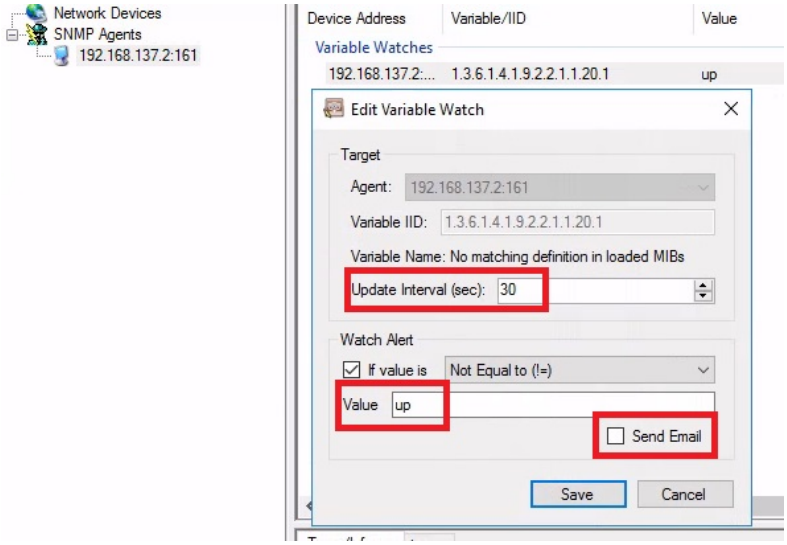


Рисунок 18 - ловушки

После отключения в консоле fastEthernet 0/0 ловушка срабатывает, после чего проверяем почту и смотрим письмо. В рисунке 19 письмо с ошибкой, что сработал трап.

```
A Variable Watch has exceeded its
configured limit:
Agent: 192.168.137.2:161
Variable: 1.3.6.1.4.1.9.2.2.1.1.20.1
The Agent's response contained a value
of administratively down, which is Not
Equal to (!=) the configured limit of
up.
```

Рисунок 19 – письмо с ошибкой

Это были настройки для SNMPv1 и SNMPv2. Данные версии настраиваются одинаково, но в них напрочь отсутствует безопасность. Те, кто задумываются о защите своих данных используют SNMPv3. Именно безопасность в первую очередь с подвигла разработчиком в создание новой

Рассмотрим настройку самой безопасной версии по рисунку 20.

```
Router(config)# snmp-server view SNMP-RO
system included
Router(config)# snmp-server view SNMP-RO
mib-2 included
Router(config)# snmp-server group
TEST v3 priv read SNMP-RO access
SNMP_ACL
Router(config)# snmp-server user ADMIN
TEST v3 auth sha cisco123 priv aes 128
snmp321
Router(config)# snmp-server enable traps
snmp
```

Рисунок 20 – настройки SNMPv3

Пояснения командам изображенных на рисунке 20:

- строка 1 – запуск SNMP-RO для OID структуры;
- строка 2 – запуск SNMP-RO для OID(mib-2);
- строка 3 – создает группу(TEST) с включением шифрования и аутентификации;
- строка 4 – в группе создается юзер админ, аутентификация по алгоритму(sha), устанавливается пароль, шифрование;
- строка 5 – типы ловушек.

В версии SNMPv3 есть три уровня безопасности они изображены на рисунке 21, а на рисунке 22 добавлены дополнительные уровни к ним.

```
R1(config)#snmp-server host 192.168.137.40 version 3 ?
  auth    Use the SNMPv3 authNoPriv Security Level
  noauth  Use the SNMPv3 noAuthNoPriv Security Level
  priv    Use the SNMPv3 authPriv Security Level

R1(config)#snmp-server host 192.168.137.40 version 3
```

Рисунок 21 – 3 уровня безопасности

Уровни безопасностей делятся на три категории:

- auth – MD5/SHA отсутствует шифрование(авторизация пользователя);
- noauth – отсутствует шифрование и аутентификация;
- priv – MD5/SHA-1 аутентификация, шифрование данных DES/3DES/AES.

Security Model	Security Level	Authentication Strategy	Encryption Type
SNMPv1	noAuthNoPriv	Community string	None
SNMPv2c	noAuthNoPriv	Community string	None
SNMPv3	noAuthNoPriv	Username	None
SNMPv3	authNoPriv	MD5 or SHA-1	None
SNMPv3	authPriv	MD5 or SHA-1	DES, 3DES, or AES

Рисунок 22 – уровни безопасности

Для применения authPriv необходима прошивка с включением криптографии(к9). Authpriv выполняет те же функции auth, но дополнительно записывает историю действий и данные пользователей в журнал, которые могут прочитать только определенные пользователи имеющие доступ. Authpriv обеспечивает максимальный уровень защищенности. Однако, есть немаловажный минус, то что сетевые устройства могут испытывать перегруз от шифрования, поэтому многие выбирают authNoPriv, стоит сказать, что уровень защиты в нем тоже высок. Остановимся на auth и пропишем нужные команды для исполнения.

Осталось настроить куда будет отправлять ловушки при его срабатывании. Вводим в консоле команды по рисунку 23.

```
R1(config)# snmp-server host
192.168.137.40 version 3 noauth ?
 WORD SNMPv1/v2c community string or
SNMPv3 user name

R1(config)# snmp-server host
192.168.137.40 version 3 noauth ADMIN -
для начала без пароля и шифрования
```

Рисунок 23 – настройка получателя ловушек

Данные о срабатываемых ловушках будет отсылать на хост 192.168.137.40. Указывается 3 версия, с отсутствием аутентификации и шифрования для юзера АДМИН.

Для проверки правильных настроек отключаем, а потом включаем один из кабелей и обращаемся к диспетчеру. В окне наблюдаются две сработанные ловушки. Как и указывалось ранее ловушки пришли без пароля и шифрования. Теперь будут настраиваться ловушки с шифрованием и паролем. Для этого

удаляем прежние настройки(ловушки). Вводим команду с теми же параметрами, только вместо noauth, указываем priv. И проверяем, отключив fastEthernet 0/0. По рисунку 24 видно, что шифрование и пароль включены.

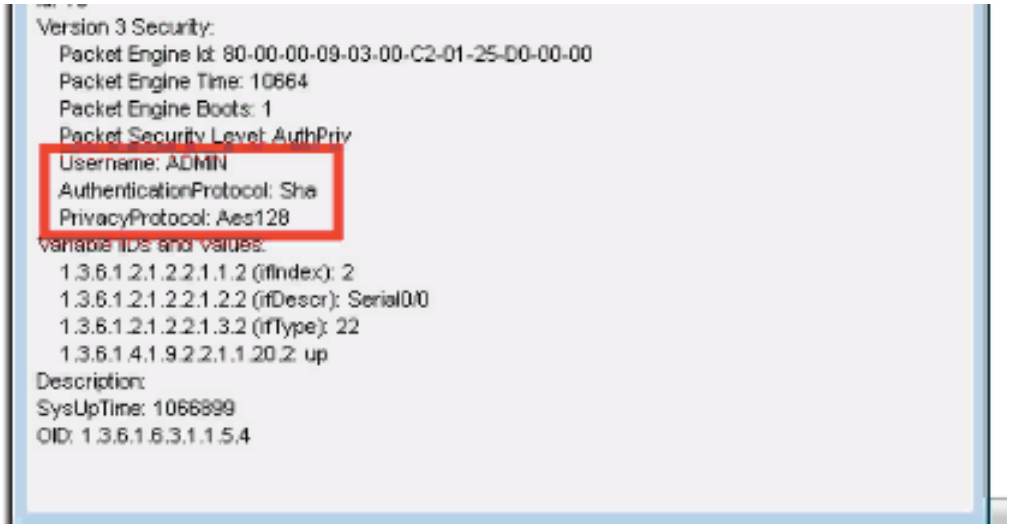


Рисунок 24 – сообщение от ловушки

Таким образом, был рассмотрен принцип работы ловушек на маршрутизаторе, который подсоединен к облаку. Использованы при этом разные уровни безопасности с разными типами шифрования и аутентификации. Убедились в удобстве и практичности его использования.

Заключение

Исходя из проделанной работы можно заключить, что протокол для мониторинга и управления SNMP успешно реализуется в сетевых устройствах.

SNMP в наше время является самым популярным протоколом и встроен во все операционные системы. Данный протокол используется в управление большими и малыми сетями. И помогает реализовывать самые разнообразные задачи в администрирование сети. При этом используется минимальный набор команд.

Можно с уверенностью заявить, что в наше время, SNMP протокол является отличным помощником администратора, который поможет не только благополучно функционировать сети, но и облегчить работу.

Библиографический список

1 Основные понятия протокола SNMP [электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/SNMP, свободный.

2 Принципы применения SNMP [электронный ресурс]. Режим доступа: http://www.codenet.ru/webmast/snmp/, свободный.

3 История создания протокола [электронный ресурс]. Режим доступа: http://citforum.ru/internet/articles/art_10.shtml, свободный.

4 Управляющая база данных MIB [электронный ресурс]. Режим доступа: http://book.itep.ru/4/44/mib44131.htm, свободный.

5 Протокол управления SNMP [электронный ресурс]. Режим доступа: http://book.itep.ru/4/44/snm_4413.htm, свободный.

6 Принципы применения SNMP [электронный ресурс]. Режим доступа: http://www.codenet.ru/webmast/snmp/, свободный.

7 Основы SNMP [электронный ресурс]. Режим доступа: http://www.k-max.name/linux/snmp-protocol/#mib, свободный.

8 Настройка ловушек на протоколе SNMP [электронный ресурс]. Режим доступа: https://arny.ru/network/nastroyka-snmp/, свободный.

9 Управление сетевой инфраструктурой по протоколу SNMP [электронный ресурс].Режим доступа: https://www.ibm.com/developerworks/ru/library/snmp_essentials_01/index.html, свободный.

10 Архитектура корпоративных сетей: учеб. Пособие / Е.В Ольков. СПб.: БХВ – Петербург, 2014. – 212 с.

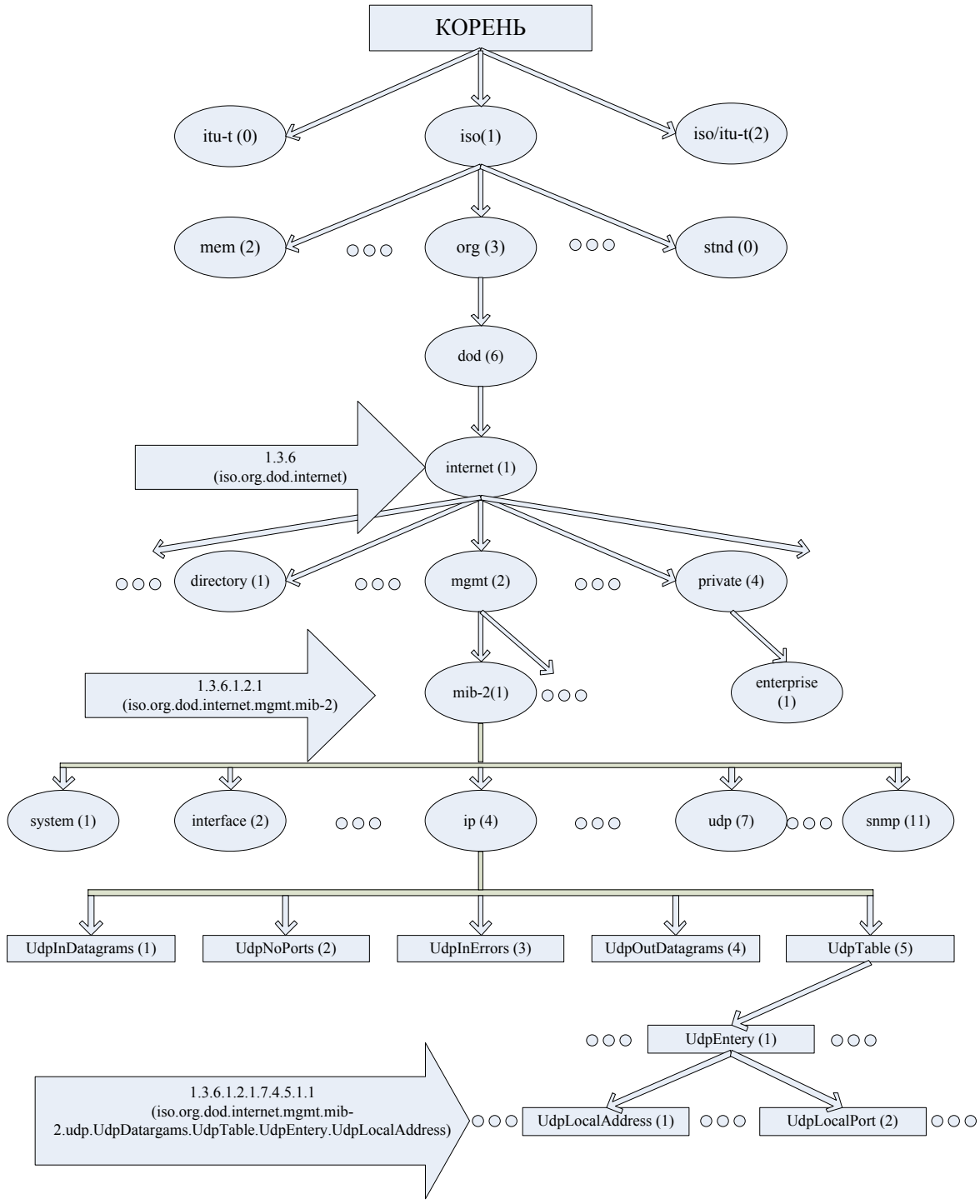
11 Сети связи: учеб. Пособие / Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский. – СПб.: БХВ – Петербург, 2014. – 400 с. ил.: – (Учебная литература для вузов)

12 СТО ЮУрГУ 04-2008 Стандарт организации. Курсовое и дипломное проектирование. Общие требования к содержанию и оформлению /

составители: Т.И. Парубочая, Н.В. Сырейщикова, В.И. Гузеев, Л.В. Винокурова. - Челябинск: Изд-во ЮУрГУ, 2008. – 56 с.

ПРИЛОЖЕНИЕ А

Дерево MIB(база управляющей информацией)



№ п/п	Формат	Обозначение	Наименование	Колич.
			Текстовые документы.	
1	А4	ЮУрГУ-Д.11.03.02.20.237.00 ПЗ	Пояснительная записка	43
			Графические материалы.	
2	А1	ЮУрГУ-Д.11.03.02.20.237.00 Д2	Настройка SNMP	1
3	А1	ЮУрГУ-Д.11.03.02.20.237.01 Д2	Уровни моделей OSI	1

Изм.	Лист	№ докум.	Подпись	Дата	ЮУрГУ-Д.11.03.02.20.237.00 Д4			
Разраб.	Хасанов И.И.				Система мониторинга цифровой сети оператора связи на основе протокола SNMP Ведомость дипломной работы	Лит.	Лист	Листов
Провер.	Новиков В.В.					Д		1
Н. Контр.	Спицына В.Д.					ЮУрГУ Кафедра ИКТ		
Утв.	Даровских С.Н.							