МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

Московский педагогический государственный университет

Институт физики, технологии и информационных систем

Кафедра технологических и информационных систем

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**БАКАЛАВРА**

на тему

«Мониторинг технического состояния сетевых устройств в образовательной организации»

Студента 4 курса

Направление подготовки: 09.03.02 Информационные системы и технологии

Профиль Информационные технологии в образовании

Тищенко Константина Константиновича

|  |  |
| --- | --- |
| Научный руководитель: | Горелко Д.С., ст.п. КТиИС |
|  |  |

|  |
| --- |
| Дипломная работа допущена |
| к защите перед Итоговой государственной |
| аттестационной комиссией |
|  |
| Заведующий кафедрой ТиИС  Нижников А.И. |

УТВЕРЖДАЮ

Заведующий кафедрой КТиИС

\_\_\_\_\_\_\_\_\_\_\_\_\_ Нижников А.И.

«\_\_\_» 20\_\_г.

**ЗАДАНИЕ**

**на разработку выпускной квалификационной работы**

студента ИФТИС

Тищенко Константина Константиновича

**Наименование темы: «Мониторинг технического состояния сетевых устройств в образовательной организации»**

**Тема закреплена приказом ректора от** «\_\_\_\_» ­­­\_\_\_\_\_\_\_\_20\_\_ г. №\_\_\_\_\_\_\_\_\_

**Целевая установка и основные вопросы, подлежащие разработке**

**при выполнении работы:**

Цель работы – Внедрение системы комплексного мониторинга сетевого оборудования в существующую инфокоммуникационную сеть образовательной организации.

**Вопросы, подлежащие разработке:**

1. *Проанализировать распространённые системы сетевого мониторинга и их компоненты.*
2. *Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети образовательной организации, построить карту сети. Определить наиболее подходящие системы мониторинга для данной инфокоммуникационной сети.*
3. *Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.*
4. *Оценить техническое состояние имеющейся сетевой инфраструктуры образовательной организации. Разработать справочную документацию к внедренной системе мониторинга.*

**Руководитель: ст.п. КТиИС, Горелко Д.С.**

«\_\_\_\_» \_\_\_\_\_\_\_\_\_20\_\_\_ г.

**Задание получил**: **Тищенко Константин Константинович**

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Оглавление

[Введение 6](#_Toc39795495)

[Глава 1. Инфокоммуникационные сети в образовательной организации 9](#_Toc39795496)

[1.1 Инфокоммуникационная сеть кафедры ТиИС МПГУ 10](#_Toc39795497)

[1.2 Исследование и анализ программных средств мониторинга инфокоммуникационной сети 15](#_Toc39795498)

[Глава 2. Практика 22](#_Toc39795499)

[Заключение 23](#_Toc39795500)

[Список литературы 24](#_Toc39795501)

[Приложение 1 25](#_Toc39795502)

## Введение

Инфокоммуникационная сеть современной образовательной организации представляет собой комплексную систему. Система мониторинга способствует стабильности работы всех узлов и оконечных устройств. Она позволяет собирать и анализировать данные с оборудования сети в одном месте. Это позволяет быстро и эффективно определять узкие места в инфокоммуникационной сети, обнаруживать скрытые дефекты, оперативно определять и устранять неисправности оборудования и как следствие поддерживать работоспособность инфокоммуникационной сети на должном уровне. Система мониторинга, развернутая в инфокоммуникационной сети, представляет собой автоматизированный процесс сбора информации различного рода с сетевых устройств, хранения данной информации и предоставление ее пользователю в удобном для него виде. Кроме того, современные системы мониторинга предоставляют возможность оперативного оповещения пользователей и/или инженеров наблюдаемой инфокоммуникационной сети.

Следует отметить, что практически все системы мониторинга, использующиеся для мониторинга инфокоммуникационных сетей, используются и в других областях. Нет принципиального значения откуда именно собирать данные – с сетевого оборудования, с производственных станков, с датчиков умного дома, датчиков транспортного средства или откуда-либо ещё.

Если говорить об актуальности данной тематики, то в 2011 году в Германии была разработана концепция развития промышленности «Индустрия 4.0», которую также называют грядущей четвертой промышленной революцией, она подразумевает под собой максимальную автоматизацию производств – интеграцию кибернетических систем в заводские процессы. С 2014 года она активно внедряется на территории всей страны, в первую очередь в тяжелой промышленности: машиностроении и автомобилестроении, являющихся локомотивами немецкой экономики. В 2014 году в Соединенных Штатах Америки был создан консорциум промышленного интернета. Для Соединенных Штатов Америки автоматизация производственных процессов стала важным национальным приоритетом. В рамках этой концепции государственные органы Соединенных Штатов Америки содействуют возвращению производства американских компаний на территорию страны, способствуют их модернизации и преобразованию в фабрики будущего. В последние годы к этим тенденциям присоединяются и другие ведущие мировые государства: Франция, Япония, Южная Корея, Китай. Уже сегодня отголоски этих процессов можно наблюдать и в повседневной жизни, например, в развитии технологий «Умного дома», трехмерной печати, печатной электроники и пр.

Обращаясь к проблематике автоматизации сбора данных в инфокоммуникационных сетях, то мониторинг сетевого оборудования позволяет в ряде случаев предупредить ошибки и выход оборудования из строя, в ряде случаев, оперативно исправить возникающие проблемы и сократить или вовсе предупредить простой в работе предприятия. Таким образом мониторинг инфокоммуникационной сети позволяет существенно сократить издержки в работе предприятия и уберечь от репутационных потерь.

Таким образом тематика автоматизации процессов в целом и автоматизация сбора данных в инфокоммуникационной сети в частности, является актуальной на сегодняшний день. В следствии этого была выбрана тема данной выпускной квалификационной работы: «Мониторинг технического состояния сетевых устройств в образовательной организации».

В ходе работы необходимо будет решить следующие задачи:

1. Проанализировать распространённые системы сетевого мониторинга и их компоненты.

2. Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети образовательной организации, построить карту сети. Определить наиболее подходящие системы мониторинга для данной инфокоммуникационной сети.

3. Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.

4. Оценить техническое состояние имеющейся сетевой инфраструктуры образовательной организации. Разработать справочную документацию к внедренной системе мониторинга.

## Глава 1. Инфокоммуникационные сети в образовательной организации

Развитие информационных технологий привело к созданию локальных вычислительных сетей и систем, а интеграция информационных технологий и телекоммуникаций привела к появлению нового термина – «инфокоммуникации».

Сам термин «Инфокоммуникации» появился лишь в начале 21 века. Инфокоммуникационные сети и технологии являются относительно новой отраслью экономики, получающей интенсивное развитие в последние годы.

Инфокоммуникационная сеть (Infocommunication Network) – это совокупность территориально рассредоточенных информационных, вычислительных ресурсов, программных комплексов управления, размещаемых в оконечных системах сети и терминальных системах пользователей, взаимодействие между которыми обеспечивается посредством телекоммуникаций, и которые совместно образуют единую мультисервисную платформу.

Инфокоммуникационные сети в образовательной организации представляют собой конвергентные сети, объединяющие в себе множество сетей, раньше являющихся раздельными, например, таких как локально-вычислительная сеть, сеть видео наблюдения, телефония, сигнализация и т.д. Объединение множества сетей в одну, хоть и является более прогрессивным решением, однако создает еще больше требований к бесперебойной работоспособности данной инфокоммуникационной сети. Построение системы мониторинга в инфокоммуникационной сети позволяет решить эту задачу.

Новый этап в развитии инфокоммуникационных сетей в образовательных организациях РФ задала Московская Электронная Школа (МЭШ). Для мониторинга построенной инфраструктуры используются сразу два решения: «Cisco Prime Infrastructure» и «Zabbix». Данные решения позволяют собирать и отслеживать все изменения внутри инфокоммуникационных сетей школ и колледжей города Москвы участвующих в программе. Оперативно реагировать на проблемы и предотвращать их возможное появление.

### Инфокоммуникационная сеть кафедры ТиИС МПГУ

Инфокоммуникационная сеть кафедры технологических и информационных систем Московского педагогического государственного университета была создана больше десяти лет назад. Для построения системы мониторинга необходимо изучить оборудование и сервисы, использующиеся в данной инфокоммуникационной сети.

В серверной стойке кафедры ТиИС МПГУ располагается следующее оборудование:

|  |  |  |  |
| --- | --- | --- | --- |
| Оборудование | Сервис | Описание | Внутренний ip-адрес |
| Сервер Kraftway Express 4EM15 | Active Directory | Active Directory («Активный каталог», AD) – решение предоставленное компанией Microsoft объединяющее различные объекты сети в единую систему. AD хранит сведения о пользователях сети кафедры ТиИС, об устройствах введенных в домен, групповых политиках и многое другое. | 192.168.0.5 |
|  | Web-server | Обслуживание адресов ftip.ru и elearning.ftip.ru | 192.168.0.254 |
|  | Маршрутизатор | В качестве маршрутизатора используется дистрибутив, основанный на FreeBSD – PFSence | 192.168.0.1 |
|  | Wi-Fi controller | Контроллер беспроводной сети производит автоматический поиск, централизованную настройку WiFi точек доступа и обновление программного обеспечения подключенных точек доступа. | 192.168.0.199 |
| Сервер Kraftway Express Lite L13 | File Server | Данный сервер предназначен для хранения файлов студентов, преподавателей и других сотрудников. | 192.168.0.3 |
| Сервер Kraftway Express Lite L13 | FreeNAS | FreeNAS – Операционная система на основе FreeBSD. Выполняет роль сетевого хранилища. | 192.168.0.4, 172.16.32.10 |
| Kraftway Express ISP ES15 | Hyper-V | Данные сервера служат для развертывания учебных виртуальных машин с помощью программного обеспечения Hyper-V. | 92.168.0.251, 172.16.32.11 и 192.168.0.252, 172.16.32.12. |
| Коммутатор Cisco Catalyst 2960G |  | Сетевое устройство, работающее на втором уровне модели OSI и осуществляющее коммутацию кадров Ethernet на основе MAC-адресов. | 192.168.0.2 |

Кроме того, в сети кафедры расположены следующие устройства:

1. Сетевой принтер Epson AcuLaser C4000, внутренний IP-адрес 192.168.0.215
2. 3 точки доступа UniFi AP служащие для подключения к инфокоммуникационной сети кафедры сети беспроводных устройств.
3. Коммутатор Cisco 2960.

Данная сеть разделена на три виртуальные локальные сети для увеличения производительности, улучшения безопасности и сокращения количества устройств в домене широковещательной рассылки.

Топологию инфокоммуникационной сети кафедры ТиИС можно увидеть на Рисунке 1 (Нарисовать получше).



Рисунок 1. Топология инфокоммуникационной сети кафедры ТиИС

В инфокоммуникационной сети кафедры Технологии и Информационных систем используются коммутаторы производства компании Cisco. Согласно информации, предоставляемой международной сетевой академии Cisco оптимальным способом, является сбор метрик посредством протокола SNMP.

SNMP – сетевой протокол для диагностики, мониторинга и управления устройств и программного обеспечения. Его спецификация описана международными стандартами RFC1155, RFC1212, RFC1213, RFC1157 и RFC3411. SNMP определён IETF (Internet Engineering Task Force) как компонент сетевой модели передачи данных TCP/IP.

SNMP работает на прикладном уровне стека OSI. Данный протокол предоставляет формат сообщения для обмена данными между агентами (управляемых узлов) и диспетчерами (управляющих узлов). Диспетчер может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Кроме того, агенты SNMP могут пересылать информацию непосредственно в систему управления сетями посредством передачи не запрашиваемых диспетчером уведомлений (ловушек, traps).

Использование ловушек обусловлено недостатками периодического опроса диспетчером агента, такими как компромисс между частотой опроса и пропускной способностью канала и снижение задержки времени между событием и его обнаружением. Чтобы избавиться от этих недостатков, агенты SNMP могут создавать и отправлять ловушки, сообщая диспетчеру о некоторых события немедленно. Примерами таких событий могут быть, смена состояния канала, попытки аутентификации пользователей, отслеживание mac-адресов и другие.

Существует несколько версий SNMP:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Модель протокола | Аутентификация | Шифрование | Результат | Описывающие документы |
| SNMPv1 | По имени сообщества | Не поддерживается | Использует проверку имени сообщества для проверки подлинности | RFC1157 |
| SNMPv2c | По имени сообщества | Не поддерживается | Использует проверку имени сообщества для проверки подлинности | RFC1901-1908 |
| SNMPv3 | По имени пользователя или посредством MD5/SHA | Возможно(DES/AES) | Использует проверку имени пользователя для проверки уровня доступа или обеспечивает аутентификацию на основе алгоритмов HMAC-MD5/HMAC-SHA | RFC2273-2275  RFC3410-3415 |

В версиях SNMPv1 и SNMPv2c для контроля доступа используется модель «Строки сообщества». Строка сообщества представляет собой незашифрованный пароль. Существует два типа строк сообщества

1. Только чтение (RO)
2. Чтение и запись (RW)

В связи с тем, что данные версии предоставляют минимальную безопасность, рекомендуется их использование только в режиме RO.

Поскольку сбор метрик является однотипной и постоянной задачей, эффективнее использовать метод сбора через ловушки, настроив агента, чем с некоторой периодичностью опрашивать агента через диспетчера. Таким образом при использовании ловушек, достаточно с точки зрения безопасности использовать SNMPv2 в режиме «только чтение» и настроить листы доступа на сетевом оборудовании, огранив доступ с других устройств.

агенты

### Исследование и анализ программных средств мониторинга инфокоммуникационной сети

Для выбора системы мониторинга оборудования в инфокоммуникационной сети, необходимо произвести исследование имеющихся на рынке решений, оценить их перспективы для решения конкретной задачи. На основе проведенного исследования необходимо выбрать наиболее оптимальное решение.

Следует отметить, что кроме программных средств мониторинга инфокоммуникационных сетей на рынке также представлены крупные компании предоставляющие специальное оборудование для данных целей, однако, на основе исследования имеющейся инфокоммуникационной сети и наличия в ней серверов для разворачивания программного обеспечения для мониторинга сети, покупка специального оборудования изначально является не целесообразной.

Оценивая же программные продукты для мониторинга инфокоммуникационных сетей, их можно разбить на составляющие:

1. База данных. База данных должна выполнять функцию хранения полученных от оборудования данных.
2. Средство сбора и записи метрик в базу данных.
3. Средство для удобного просмотра полученных данных сетевым инженером.
4. Средство анализирующее приходящие метрики и оперативно уведомляющее ответственных лиц о выявляемых проблемах в работе оборудования инфокоммуникационной сети.

Выбор базы данных и системы управления базой данных для хранения метрик, представляет собой отдельную задачу. Для систем мониторинга инфокоммуникационных сетей наиболее распространены реляционные базы данных. Учитывая особенности данной образовательной организации наиболее всего подходят распространенные системы управления реляционными базами данных, например, такие как MySQL, PostgreSQL, MariaDB, это связано с большой популярностью языка SQL и большим количеством специалистов, умеющих с ним работать. Использование реляционных баз данных позволит обеспечить простоту поддержки системы мониторинга в будущем, например, при необходимости развития инфокоммуникационной сети и добавлении новых устройств и получаемых метрик.

Однако, следует отметить, что в последнее время среди систем мониторинга инфокоммуникационных сетей набирают популярность базы данных временных рядов (time series database/TSDB). Это базы данных, специально предназначенные для обработки информации, связанных со временем. Реляционные базы данных представляют собой таблицы, где каждая строка определяет отдельную запись. Такие таблицы и строки можно использовать для хранения абсолютно различной информации. Они эффективны в разных областях. Базы данных временных рядов устроены несколько иначе. В отличии от реляционных баз данных, данные в которых многомерны, в базах данных временных рядов данные агрегируются по времени. С течением времени и возрастанием размеров реляционной базы данных скорость приема и записи данных падает, это связано с тем, что при добавлении или удалении записи в реляционную базу данных, система управления базой данных многократно переиндексирует данные, для быстрого и эффективного доступа к ним. В итоге, при росте объемов хранимых данных производительность таких баз данных снижается. Базы временных рядов не имеют этого недостатка. Тем не менее, это этот тип баз данных, являющийся довольно перспективным, но на данный момент всё ещё представляет собой новый продукт на рынке и как следствие недостаточно оттестирован и имеет проблемы со стабильностью.

Отдельно стоит рассмотреть такие расширения как TimescaleDB и PipelineDB для системы управления базой данных PostgreSQL. Эти расширения позволяют использовать PostgreSQL вместе с базами данных временных рядов. Это позволяет использовать преимущества баз данных временных рядов вместе с проверенной временем PostgreSQL и таким образом нивелировать основной недостаток баз данных временных рядов.

Распространённые наборы программного обеспечения для мониторинга инфокоммуникационных сетей.

Zabbix – одна из самых распространенных универсальных систем мониторинга. Активно развивается с 1998 года, с 2001 года распространяется публично под лицензией GNU GPL, для хранения данных использует MySQL, PostgreSQL, SQLite, Oracle DB, IBM DB2. Имеет веб-интерфейс, написанный на PHP. Поддерживает различные виды мониторинга, как с помощью агентов, так и без. В связи с сильной распространённостью обладает крупным сообществом разработчиков и как следствие активно развивается. Используется в образовательной сфере в РФ совместно с Cisco Prime Infrastructure для мониторинга и управления оборудованием Московской Электронной Школы.

InfluxData (Стэк TICK) – Набор программного обеспечения, написанного на языке Go. Включает в себя такие программные продукты как:

1. Telegraf – собирает метрики временных рядов.
2. InfluxDB – самая распространённая база данных временных рядов. Возможна кластеризация.
3. Chronograf – программное обеспечение позволяющее визуализировать данные из базы данных временных рядов.
4. Kapacitor – отвечает за обработку полученных данных, контролирует отклонения и оповещает инженеров.

Prometheus – комплект программного обеспечения с открытым исходным кодом построенного вокруг и включающее в себя TSDB – “Prometheus”.

1. TSDB – “Prometheus”
2. Сервер, собирающий метрики и сохраняющий их в TSDB.
3. PROMDASH – Программное обеспечение для визуализации данных.
4. AlertManager – Менеджер уведомлений.
5. Pushgateway – компонент сбора метрик с краткоживущих процессов.
6. Экспортеры данных из сторонних приложений, а также набор библиотек для различных языков программирования.

Cisco Prime Infrastructure – система мониторинга и управления проводными и беспроводными инфокоммуникационными сетями. Разрабатывается и поддерживается компанией Cisco. Данное программное обеспечение позволяет выполнять мониторинг, резервное копирование и восстановление конфигураций, собирать базовую статистику с оборудования, данных инвентаризации, настраивать оборудование, выполнять контроль работы приложений, выполнять автоматическую установку оборудования без использования консольного доступа, составлять отчеты о сбоях и оперативно оповещать сетевых администраторов сети. Сбор данных с оборудования осуществляется посредством протоколов SNMP и Syslog. Так же отличительной особенностью является наличие приложения для мобильных устройств в то время как большинство систем мониторинга используют только веб-интерфейс и доступ через консоль. В образовательной сфере в РФ активно используется при мониторинге Московской Электронной Школы. Одним из основных минусов данной системы мониторинга является стоимость и закрытость исходного кода.

IBM Trivoli Monitoring – Решение от компании IBM с закрытым исходным кодом. Состоит из следующих компонентов:

1. Trivoli Enterprise Monitoring Server (TEMS) – сервер мониторинга, собирает данные с оборудования и записывает их в базу данных.
2. База данных – место хранения накопленных метрик. IBM Trivoli Monitoring допускает использование – DB2, MySQL, Oracle, Derby.
3. Tivoli Enterprise Portal Server (TEPS) – сервер предоставляющий визуальный доступ к собираемым данным.
4. Tivoli Enterprise Management Agent (TEMA) – управляемые системы (агенты), отвечают за накопление метрик с оконечного оборудования и пересылку полученных данных на TEMS. Можно разделить на два подвида: Агенты операционной системы и Агенты приложений.

Сильными сторонами данной системы являются надежность и стабильность работы, возможности масштабирования и поддержки. Слабой – стоимость и закрытость исходного кода, отсутствие поддержки TSDB.

Cacti – открытое программное обеспечение. В основе лежит кольцевая база данных (RRD) основанная на MySQL. В основе визуальной части лежит набор утилит RRDtool. Сбор данных осуществляется по протоколу SNMP. Используется как легковесное решение для маленьких конвергентных сетей, плохо поддается масштабированию не имеет агентов.

Nagios – программное обеспечение с открытым исходным кодом, позволяет наблюдать распространённые сетевые службы, состояние хостов, имеет возможность удаленного мониторинга по средством SSH и SSL. Использует агенты(плагины) для сбора данных. Имеет встроенный графический интерфейс. Основным недостатком Nagios является сложность настройки и дальнейшей поддержки – отсутствие web-интерфейса (в бесплатной версии) и большое количество конфигурационных файлов, связь между которыми происходит напрямую, что не позволяет оперативно и просто обнаруживать ошибки при настройке и создает дополнительные трудности в последующей поддержке и при масштабируемости.

Icinga 2 – является форком Nagios, унаследовавший основной недостаток системы мониторинга Nagios: сложная изначальная настройка даже самой простой распределенной схемы.

OpenNMS – Программная платформа для мониторинга, построенная на событийно-ориентированной архитектуре, не имеет агентов, поддерживает работу с популярной информационной панелью grafana. Имеет встроенные модули формирования отчетности, поддерживает Linux, Windows, Solaris и OSX. Имеет как собственную настраиваемую информационную панель администратора, так и поддержку такого открытого программного обеспечения как Grafana. Одним из недостатков является слабая документация и малая распространённость на территории РФ. Слабая популярность данной системы мониторинга среди малого бизнеса вызвана высокой ценой поддержки и «заточенностью» под сети крупных размеров.

Отдельно в качестве средства для визуализации и анализа получаемых данных стоит рассмотреть продукт open-source сообщества с открытым исходным кодом – Grafana. Данный продукт имеет возможность получать данные как из всех распространённых баз данных, так и напрямую из множества программных продуктов, собирающих метрики и записывающих их в базы данных. Стоит отметить, что он поддерживает все распространённые системы мониторинга и базы данных. Наличие большого количества документации, удобство интерфейса и визуальной составляющей делает его безусловным лидером на рынке, в качестве альтернативы можно рассматривать встроенные во многие системы мониторинга продукты, но большинство из них не обладают всеми возможностями Grafana. Кроме всего прочего Grafana имеет встроенные возможности для настройки триггеров на события и различные варианты оповещения сотрудниках как уже о случившихся сбоях в работе инфокоммуникационной сети, так и о предполагаемых проблемах в будущем.

*Вывод:*

На основе проведенного анализа, было принято решение для построения системы мониторинга использовать следующий набор:

В качестве сборщика метрик использовать Zabbix 4.4 со следующим набором компонентов, при этом заменить web-сервер, используемый по умолчанию на nginx, в качестве базы данных использовать PostgreSQL с расширением TimescaleDB и PipelineDB. В качестве средства визуализации данных и оповещения о нестандартных ситуациях вместо встроенного в Zabbix веб-интерфейса использовать продукт open-source сообщества – Grafana.

## Глава 2. Практика

## Заключение

## Список литературы

25 наименований

1. Воробиенко, П.П. Инфокоммуникации: термины и определения [Текст] / П.П. Воробиенко, Л.А. Никитюк // Научный журнал «Восточно-Европейский журнал передовых технологий» //. - Харьков: Технологический центр, 2011. - №6/2 (54), с. 4-6.
2. Новая парадигма промышленного развития Германии. Стратегия «Индустрия 4.0» URL: https://cyberleninka.ru/article/n/novaya-paradigma-promyshlennogo-razvitiya-germanii-strategiya-industriya-4-0/viewer (Дата обращения: 16.09.2019)
3. Ссылку на мою статью с Д.С. Горелко о МЭШ
4. Ссылки на RFC к SNMP

## Приложение 1

Настройка оборудования Cisco

1. Настройка строки сообщества и уровень доступа («Только чтение» или «Чтение и запись»):

snmp-server community *string* ro | rw

1. Назначьте получателя ловушек:

snmp-server host *ip* [version{1| 2c | 3 [auth | noauth | priv]}] *community-string*.

3) Включите ловушки на агенте SNMP

snmp-server enable traps *notification-types*

Без указания типа ловушек – будут отправляться все.

(Примечание. По умолчанию в SNMP не установлены ловушки. Без этой команды диспетчеры SNMP должны будут проводить опрос для получения всей существенной информации.)

Дополнительно:

Настройка местоположения устройства:

snmp-server location *text*

Зафиксируйте системный контакт:

snmp-server contact *mail@gmail.com*

Ограничение доступа по SNMP:

ip access-list standard *NAME*

permit *ip*

snmp-server community *string* ro | rw *NAME*

Просмотр настроек:

show snmp

show snmp community