|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

**Институт информационных технологий (ИТ)**

**Кафедра инструментального и прикладного программного обеспечения (ИиППО)**

**КУРСОВАЯ РАБОТА**

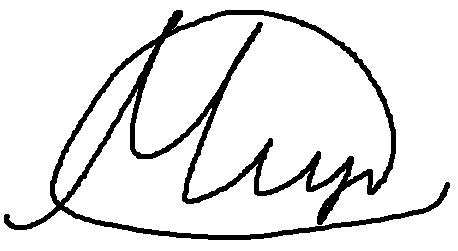
по дисциплине: Программное обеспечение локальных сетей

направления профессиональной подготовки: 09.03.04 «Программная инженерия»

Тема: Анализ сетевого трафика с помощью программы PRTG

Студент: Миронов Алексей Дмитриевич Группа: ИКБО-02-19

Работа представлена к защите (дата) /Миронов А.Д./



(подпись и ф.и.о. студента)

Руководитель: ассистент, Лепёхин Владимир Викторович

Работа допущена к защите (дата) /Лепёхин В.В./

(подпись и ф.и.о. рук-ля)

Оценка по итогам защиты:

/ /

/ /

(подписи, дата, ф.и.о., должность, звание, уч. степень двух преподавателей, принявших защиту)

М. РТУ МИРЭА. 2021 г.

**СОДЕРЖАНИЕ**

1. Введение………………………………………………………….….....3
   1. Цель………………………………………………………………....3
   2. Предназначение программы PRTG…..………………...................3
2. Общее описание исследуемого ПО………………………………...…3
3. Описание реализаций на основе исследуемого ПО………………...14
4. Заключение……………………………………………………………20
5. Список использованных информационных источников…………………………………………………………….20

**Перечень сокращений**

PDF - Portable Document Format — формат электронных документов

PRTG - Paessler Router Traffic Grapher

IT - Information Technology

API - application programming interface

WMI - World Manufacturers Identification — всемирный индекс изготовителя

УЗ - Учетная запись

DNS - Domain Name System — система доменных имён

1. **Введение**

В наше время практически все компании используют интернет для различных нужд. Будь то крупные IT корпорации или даже салоны красоты. Часто в компаниях бывает много тысяч сотрудников и тогда количество трафика и его назначение становится трудно отследить. Для этих целей были созданы программы для контроля трафика. Сейчас их довольно много и одно из самых популярных – PRTG.

* 1. **Цель**

Данная работа проведена с целью изучения работы программы PRTG, а также её особенностей и сфер применения. В данной работе будут разобраны такие вещи как: Интерфейс программы PRTG, различные методы настройки и использования. А также некоторые примеры реального применения данной программы

* 1. **Предназначение программы PRTG**

Данная программа предназначена для мониторинга , визуализации и контроля использования сети.

1. **Общее описание исследуемого ПО**

Ключевыми особенностями программы PRTG являются следующие факторы:

* 1. **Производительность**

Большие установки способны довольно значительно нагружать систему мониторинга. В результате проблем с производительностью, вызванных высокими нагрузками, часто появляются искажения в результатах мониторинга. Зачастую это приводит к недовольству пользователей. Повышается риск отказов и сбоев. Программа PRTG может довольно неплохо справляться с высокими нагрузками, и может предлагать оптимальные стратегии для избежания проблем с производительностью.

**2.2 Совместимость**

Системы мониторинга могут являться центральными компонентами ИТ-инфраструктуры, поэтому важным фактором является то, что система мониторинга должна быть совместима со сторонними решениями. Программу PRTG можно совместить с устройствами и программами от любых производителей, многофункциональный API дает возможность создавать необходимые решения для мониторинга.

**2.3 Распределенные среды**

Большая инфраструктура сети может включать в себя несколько локальных сетей. С помощью PRTG можно создать простое решение для управления распределенным мониторингом и поддержкой. Это даёт полный обзор всех сетей инфраструктуры и помогает избежать проблем с распределением зон ответственности между сотрудниками и подразделениями.

Данная программа имеет несколько интерфейсов, среди них Web-интерфейс и desktop.

В данном случае показан вход в систему через Web-интерфейс. Его можно использовать как с компьютера, так и с мобильного устройства или же с любого другого устройства, поддерживающего Web интерфейсы. Данная система поддерживает доменные учетные записи, однако учетную запись можно создать вручную.

После входа появится экран приветствия (Рис. 1):

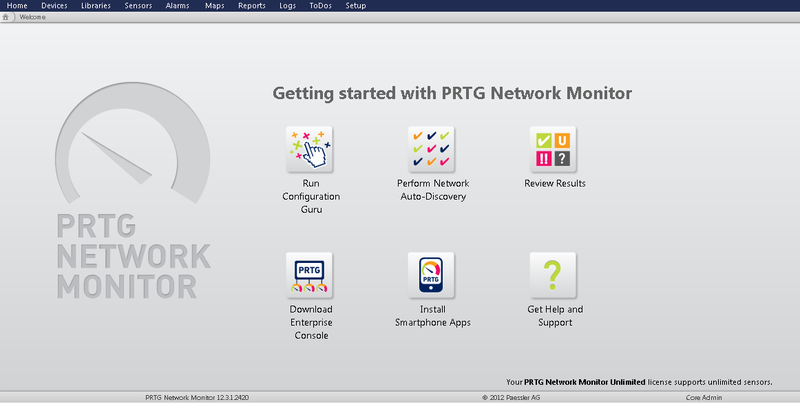


Рис. 1 Экран приветствия

При первоначальном входе в систему рекомендуется пройти по ссылке «Run Configuration Guru» которая поможет сразу же настроить большинство изначальных конфигураций (Рис. 2):

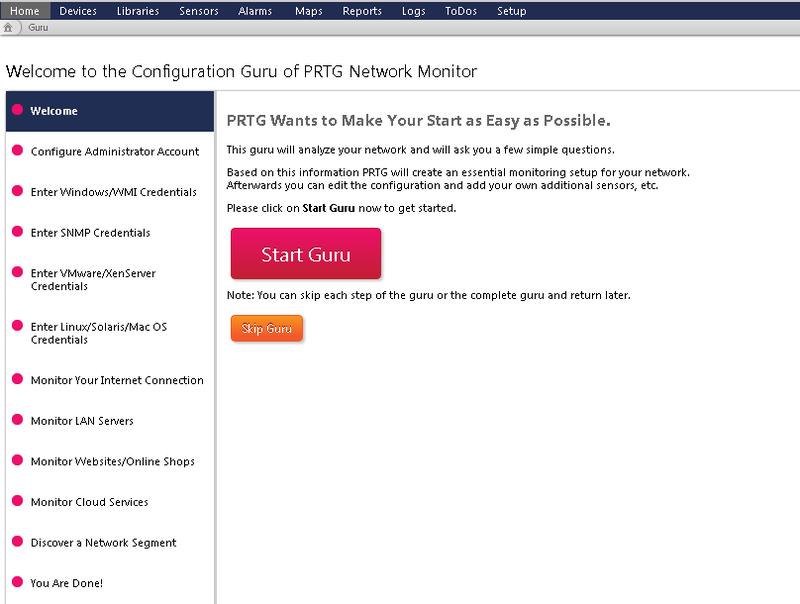


Рис. 2 Настройка конфигураций

На этой странице можно настроить следующие параметры:

• Логин и пароль корневого аккаунта администратора (core admin)

• Данные для использования с WMI сенсорами (зачастую это учетная запись, которая имеет администраторские полномочия в домене)

• При использовании UNIX или LINUX системы, так же можно прописать данные ваших УЗ.

• Данные для соединения с интернетом (например, в случае, если организация использует proxy-сервер) — доступ к интернету полезен как минимум тем, что с его помощью можно активировать систему без отправки на почту компании paessler кодов, а напрямую, но и конечно же при хорошей скорости интернета программа может самостоятельно скачивать и устанавливать обновления.

• Поиск персональных компьютеров, серверов и прочего периферийного оборудования в автоматическом режиме (если сеть или сегмент сети небольшой и не будет искаться несколько сотен машин).

После базовой настройки откроется окно, на котором отображаются все ваши устройства и сенсоры (Рис. 3):

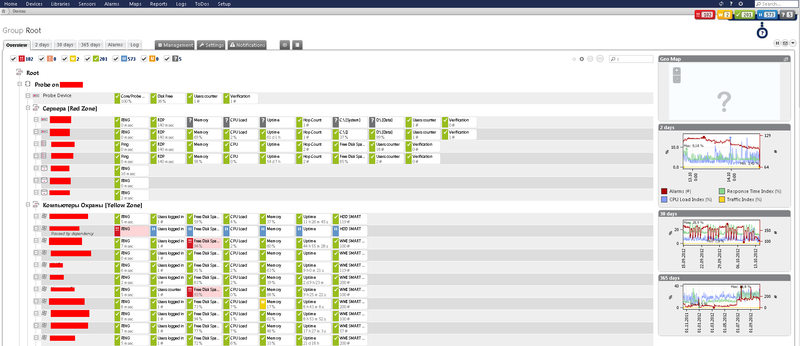


Рис. 3 Окно сенсоров

В этом окне можно увидеть множество цветовых индикаторов, которые означают следующее:

* **Красный** — ошибка \ недоступно \ превышение заданного параметра \ недостаток до заданного параметра
* **Оранжевый** — нетипичное поведение сенсора (Пример: Пинг в данный момент 200 ms, при среднем пинге на данном устройстве в данное время дня \ недели 110 ms)
* **Желтый** — предупреждение (сенсор приближается к критичных границам заданного параметра или же стал недоступен в момент прошлой проверки)
* **Зеленый** — штатное поведение сенсора
* **Синий** — пауза (устанавливается либо вручную, либо автоматически). В паузу сенсор может поставить как администратор, так и сама система по нескольким причинам: главный для устройства сенсор недоступен и все остальные сенсоры устройства установлены в режим паузы; слишком большое количество запросов одновременно — сенсор будет перезапущен после получения данных с других сенсоров.
* **Серый** — не получены данные с сенсора (только включили, только закончился режим паузы)

В данном примере рассмотрен один из вариантов решения в помощью PRTG для нового добавленного компьютера (Рис. 4):

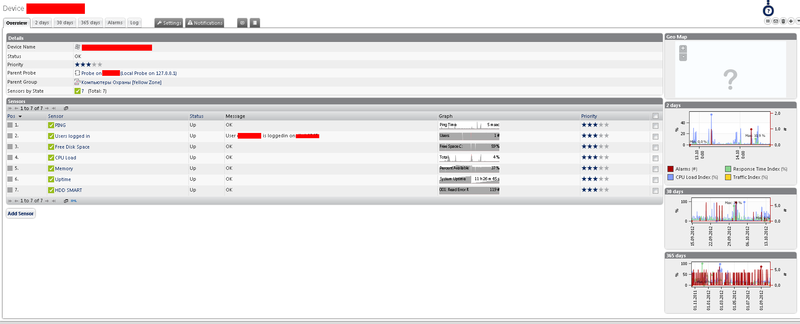


Рис. 4 Интерфейс добавления компьютеров

В этом окне можно увидеть несколько строчек описывающих состояние устройства, которые означают:

* **Ping** — стандартный ping до машины. Главный сенсор на устройстве.
* **Users logged in** — кто залогинен на данной конкретной машине.
* **Free Disk Space** — % свободного места на жестком диске.
* **CPU Load** — % загруженности процессора(-ов).
* **Memory** — % использования памяти.
* **Uptime** — время с момента последней перезагрузки ПК. Установлено ручное предупреждение — свыше 14 дней — оповещать администратора.
* **HDD Smart** — проверки нескольких параметров чтения \ записи жесткого диска.

Существует 2 варианта представления устройства в системе:

1. Группировка сенсоров внутри устройств
2. Режим карты — пользователь сам рисует \ моделируете карту расположения своих устройств для более удобного визуального восприятия (Рис. 5).

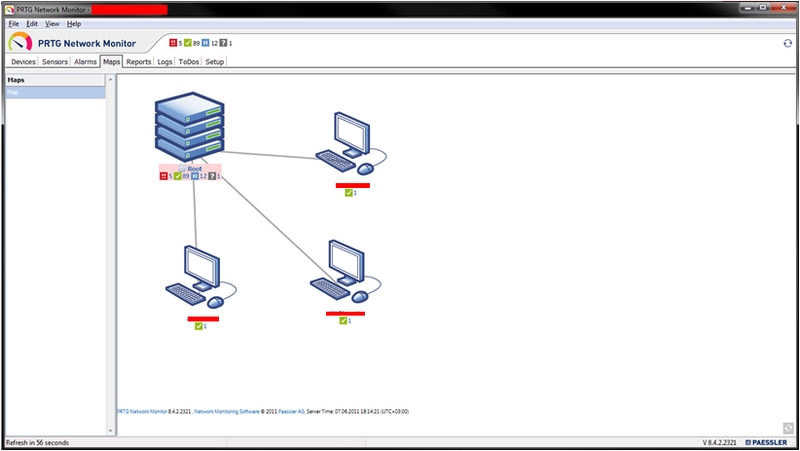


Рис. 5 Режим карты

На данный момент в системе доступно множество различных сенсоров (Рис. 6)

Сенсоры можно разделить на следующие условные категории:

• Common Sensors

• Bandwidth Monitoring Sensors

• Web Servers (HTTP) Sensors

• SNMP Sensors

• Windows/WMI Sensors

• Linux/Unix/OS X Sensors

• Virtual Servers Sensors

• Mail Servers Sensors

• SQL Database Servers Sensors

• File Servers Sensors

• Various Servers Sensors

• VoIP and QoS Sensors

• Hardware Parameter Sensors

• Custom Sensors

Меню добавления сенсоров (с версии 11 и выше):

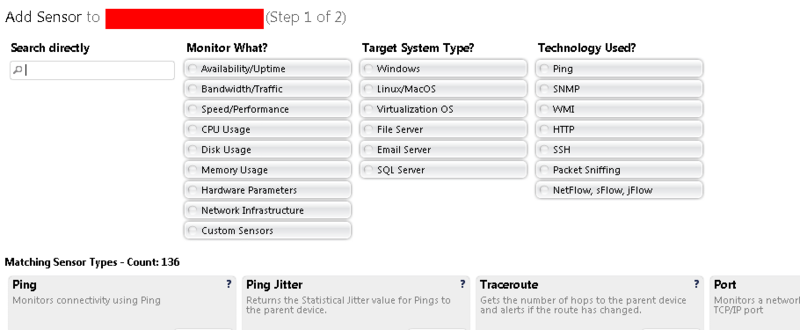


Рис. 6 Меню сенсоров

Сенсор можно найти несколькими способами:

1. Выбрать категорию и из нее выбрать нужный сенсор.
2. Найти нужный сенсор в списке снизу
3. Ввести часть названия сенсора и выбрать из предложенных вариантов.

Зачастую в реальных задачах используются далеко не все сенсоры. Всего нескольких десятков сенсоров будет достаточно для полного контроля устройства.

Программа также может формировать отчеты в автоматическом режиме.

Пример ежемесячного регионального отчета (Рис. 7):



Рис. 7 Интерфейс настройки отчетов

В данном случае отчет установлен в автоматический режим, однако у пользователя есть возможность ручного запуска процесса.

Существует 3 основные опции выпуска отчетов:

1. Просмотр в онлайн режиме html страницу с отчетом.
2. сохранить отчет в виде PDF файла на сервере и уведомить об окончании формирования отчета по почте
3. Отправить сам PDF файл конечному пользователю

На вкладке **Stored Reports** можно увидеть все сохраненные на диске файлы.

При сохранении отчета в PDF, то выглядеть он будет примерно следующим образом (Рис. 8):



Рис. 8 Пример отчета

В данном случае использовано графическое представление данных. Если необходимо получить конкретную информацию, то можно формировать отчеты в текстовом виде в разрезе, например 5 минут. Тогда можно получать вместо картинки строки вида:

«01.01.2012 09:00:00 — 01.01.2012 09:05:00 Ping 100% Available»

Большинство отчетов достаточно настроить только 1 раз, протестировать его и больше не возвращаться к нему.

Программа PRTG также обладает функционалом логирования. Логируется абсолютно сё, начиная от поведения сенсоров, заканчивая Формированием отчетности, которая в последующем будет отправлена в смс сообщении или выслана на электронную почту.

Пример лога (Рис. 9):

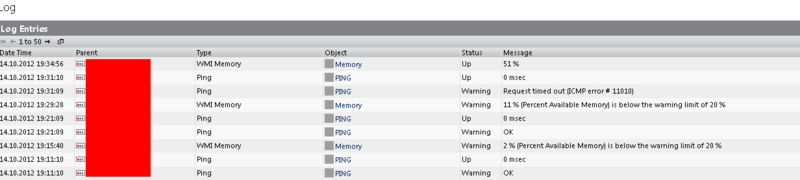


Рис. 9 Пример лога

Интерфейс логов интуитивно понятен и прост в использовании. Цветовые маркеры сигнализируют о критичности события.

1. **Описание реализаций на основе исследуемого ПО**

Несколько примеров использования PRTG в реальных задачах:

Первый пример – поиск нарушителей.

Нарушителем в данном конкретном случае считается любой пользователя, который не является владельцем конкретного устройства.

Для поиска нарушителя будет использоваться 2 сенсора типа Users logged in. Первый сенсор будет отображать реальную картину — кто в данный момент выполнил вход на машину (и выполнил ли вход вообще), а второй сенсор будет иметь на себе фильтр с логинами разрешенных сотрудников (т.е. эти логины не будут отражаться).

На второй сенсор устанавливается оповещение — если количество пользователей больше 0, то немедленно оповестить администратора по почте. Логин нарушителя отправится в письме вместе с именем и IP адресом машины, куда сотрудник пытался зайти.

Данных способ хорошо себя показывает в случае, если необходимо оперативно проверять тех, кто выполнял вход на устройство.

Второй пример:

PRTG Network Monitor и NetPing SMS для отправки SMS-уведомлений на основе SNMP TRAP сообщений

Для реализации вышеописанного функционала необходимы:

1. шлюз для отправки и приёма SMS команд NetPing SMS с установленной SIM картой;
2. настроенная система мониторинга PRTG Network Monitor

Мы рассмотрим только 2-й пункт.

Для того, чтобы настроить SMS-уведомление в системе мониторинга PRTG, необходимо перейти по вкладке «Setup» в основные настройки системы (Рис. 10):

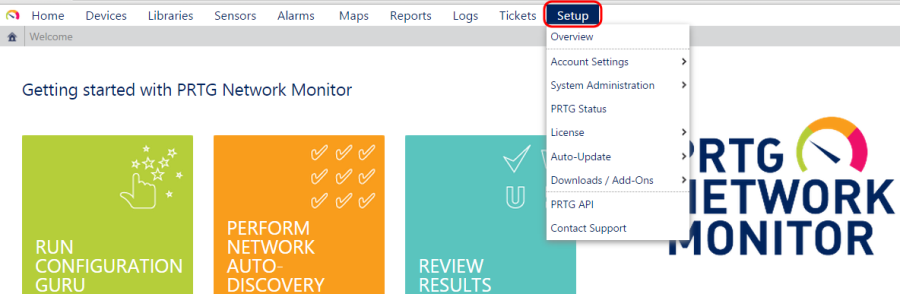


Рис. 10 Настройка системы

Переходим во вкладку «Notifications» (Рис. 11):

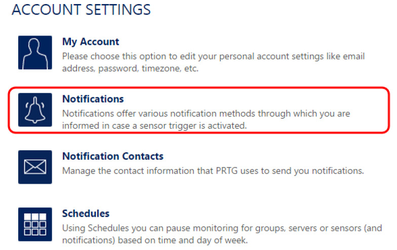


Рис. 11 Вкладка Notifications

Для получения доступа к странице «Notifications» необходимо ввести имя пользователя и пароль администратора системы (Рис. 12):

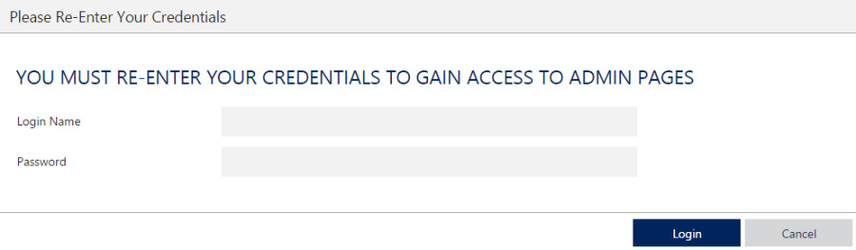


Рис. 12 Окно входа

После авторизации появится таблица «NOTIFICATIONS», в которую нужно добавить новое уведомление при помощи кнопки «Add new notification» (Рис. 13):

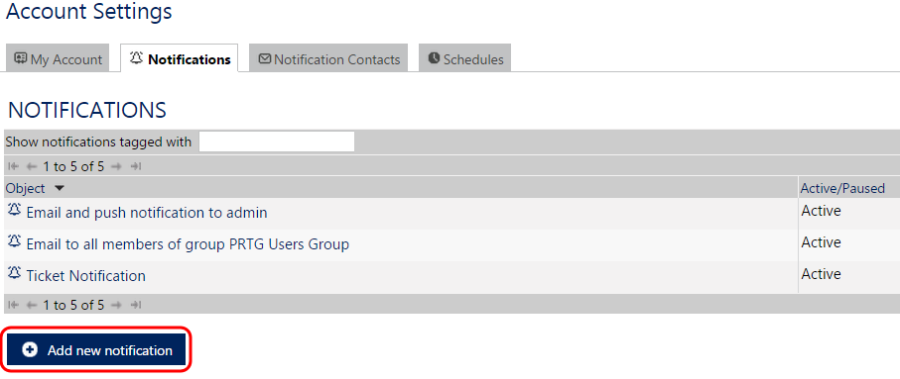


Рис. 13 Кнопка «Add new notification»

В окне настройки нового уведомления «Add notification» указать название уведомления в поле «Notification Name» и нажать чек-бокс «SEND SNMP TRAP». В области настройки «SEND SNMP TRAP» требуется заполнить параметры для отправки SNMP trap сообщений на шлюз NetPing SMS. (Рис. 14)



Рис. 14 Заполнение параметров SNMP

* **Нost/IP** – IP адрес или DNS имя компьютера, на который будут отправляться SNMP trap сообщения;
* **SNMP Port** – номер UDP порта для trap сообщений. По умолчанию: 162;
* **Commutity String** – значение Community при доступе к устройству по протоколу SNMP;
* **Specific Trap Code** – целое значение, которое поможет идентифицировать trap. По умолчанию: 0;
* **Message ID** – идентификатор, который позволяет определить оригинальный trap;
* **Message** – информационное сообщение о состоянии датчика или устройства;
* **Agent IP** – IP адрес агента. Оставить поле пустым для использования IP адреса собственного PRTG сервера

После того, как все параметры нового уведомления будут заполнены заполнения необходимо сохранить настройки нажатием кнопки «Save».

В результате этих действий новое уведомление появится в таблице «Notification» (Рис. 15):

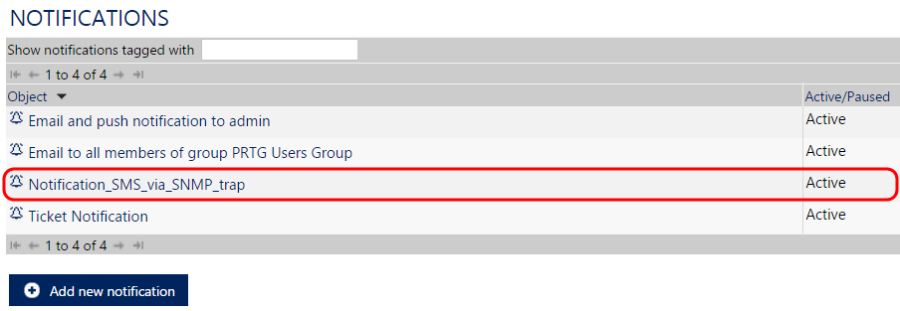


Рис. 15 Новое уведомление

Для того, чтобы созданное SMS-уведомление работало, его нужно применить к необходимым сенсорам или устройствам в системе PRTG.

Ниже приведен пример использования SMS-уведомления, которое будет срабатывать при пропадании и появлении устройства в локальной сети. Для этого нужно выбрать необходимое устройство в PRTG, которое проверяется на доступность командой «Ping». Выбор производится на странице «Devices» (Рис. 16):

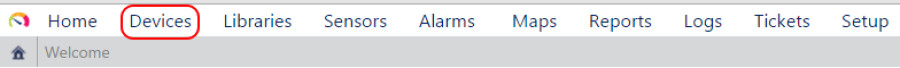


Рис. 16 Кнопка Devices

На странице «Devices» из списка устройств, настроенных на мониторинг, для примера выберем устройство «NetPing\_device». Выбор осуществляется нажатием курсора мыши по названию устройства (Рис. 17):

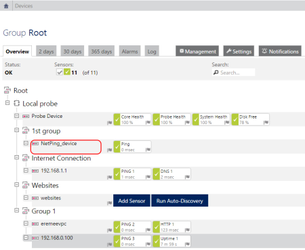


Рис. 17 Выбор устройства

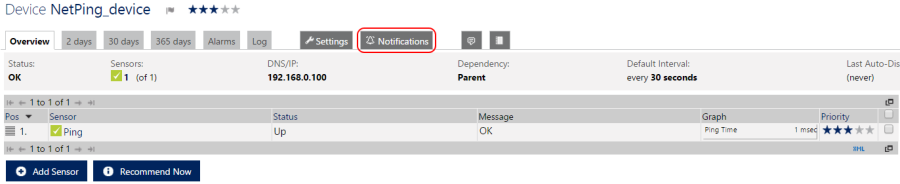
Откроется страница «Device NetPing\_device», в которой перечислены все сенсоры данного устройства. Как видно из скриншота ниже устройство «NetPing\_device» настроено только на проверку доступности посредством команды «Ping». Для применения созданного уведомления «Notification\_SMS\_via\_SNMP\_trap» необходимо перейти на вкладку «Notifications»(Рис.17):

Рис. 18 Вкладка Notifications

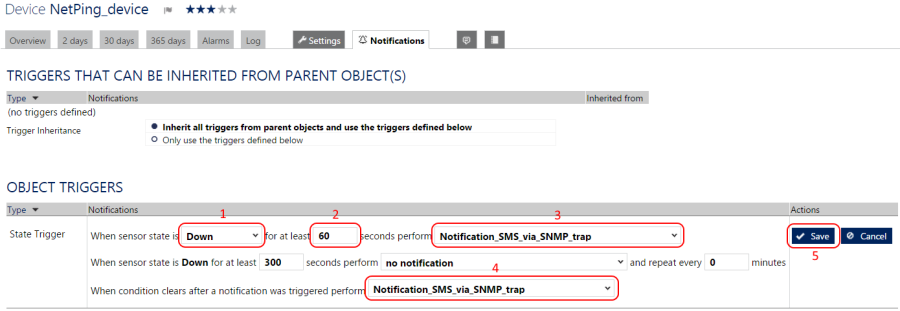
На вкладке «Notifications» настраивается реакция на изменение статуса сенсоров выбранного устройства. Для получения SMS-уведомления при изменении состояния сенсора «Ping» необходимо добавить триггер нажатием кнопки «Add State Trigger» (Рис. 17) и заполнить соответствующие поля:

Рис. 19 Настройка SMS уведомлений

где:

1 – условие при котором будет вызвано уведомление. В этом примере триггер будет активирован, когда сенсор находится в состоянии «Down»;

2 – интервал времени, через который сработает триггер. Этот интервал позволяет избежать ложных срабатываний;

3 – метод отправки уведомлений при срабатывании триггера;

4 – метод отправки уведомлений, когда условие перестает выполняться;

5 – сохранение параметров триггера

На этом настройка PRTG окончена.

На этом примере подробно разобрана настройка PRTG для конкретной задачи.

1. **Заключение**

В данной курсовой работе был рассмотрен основной функционал программы PRTG и некоторые примеры его применения. Также были разобраны основные режимы работы и интерфейсы этих режимов. Были изучены различные типы сенсоров и способы их применение. Произведено ознакомление с принципом работы программ анализа и контроля траффика различных сетей, способы использования и их предназначение.

**Список использованных информационных источников:**

1. Интернет-ресурс [URL]: https://ru.wikipedia.org/wiki/PRTG (Дата обращения: 07.05.2021).
2. Интернет-ресурс [URL]: https://www.ru.paessler.com/prtg (Дата обращения: 07.05.2021).
3. Интернет-ресурс [URL]: https://www.paessler.com/manuals/prtg/available\_sensor\_types (Дата обращения: 08.05.2021).
4. Интернет-ресурс [URL]: https://habr.com/ru/post/154747/ (Дата обращения: 09.05.2021).
5. Интернет-ресурс [URL]: https://networkguru.ru/8-luchshikh-programm-dlia-analiza-setevogo-trafika/ (Дата обращения: 07.05.2021).
6. Интернет-ресурс [URL]: http://www.netping.ru/Blog/primer-nastrojki-prtg-network-monitor-i-netping-sms-dlya-otpravki-sms-uvedomlenij-na-osnove-snmp-trap-soobshhenij/ (Дата обращения: 08.05.2021).