УДК 621.395:004.922

SNMP – ПРОТОКОЛ МОНИТОРИНГА И КОНТРОЛЯ ДЛЯ VoIP СЕТЕЙ

Г. Б. ЖИГУНОВ
(Представлено: канд. техн. наук, доц. Д. А. ДОВГЯЛО)

Актуализирована проблема управления и мониторинга IP-телефонии. Рассмотрен протокол сетевого управления локальными сетями SNMP. Показано место протокола в настройке VoIP сетей.

SNMP (Simple Network Management Protocol – простой протокол сетевого управления) крайне необходим в настройке, управлении и обеспечении безопасности IP-телефонии. SNMP собирает информацию о сети и подключенных к ней устройствах, а также обрабатывает и показывает в кратком и понятном формате. Наиболее важные аспекты VoIP, которые можно отслеживать с помощью данного протокола:

- Используемые полосы пропускания на основных и распределительных сетевых линиях;
- Состояние и работа механизмов обеспечения качества обслуживания (QoS);
- Индикация перегрузки сети по каналам сети интернет;
- Количество активных голосовых вызовов на голосовых шлюзах внутри сети;
- Состояние регистрации голосовых шлюзов и IP-телефонов;
- Измерение параметров, влияющих на ухудшение качества голосовой связи.

SNMP-менеджер может быть специально сконфигурирован таким образом, чтобы предоставлять наиболее релевантную информацию для конкретных приложений.

Поскольку данный протокол поддерживается практически всеми сетевыми устройствами, никаких сложных конфигураций не требуется. Его можно легко включить на всех устройствах, которые нужно отслеживать, и при простой настройке вся собранная информация может быть направлена на сервер мониторинга SNMP, где она собирается, обрабатывается, интерпретируется и представляется администратору.

SNMP настраивает мониторинг доступности обнаруженных VoIP-приложений, сетевых служб и процессов. Данный мониторинг осуществляется путем периодической отправки SNMP-запросов управляемым VoIP-устройствам для получения статуса приложения, сетевой службы и процессов. В таблице 1 приведен список параметров для опроса VoIP.

Таблица 1. – Список параметров для опроса VoIP [1]

Параметр	Значение по умолчанию	Описание
AnalysisMode (режим мониторинга)	ENABLED, DISABLED По умолчанию: ENABLED	Включает или отключает опрос доступности устройств для подключения.
PollingInterval (Интервал опроса)	От 30 до 3600 с По умолчанию: 240 с	Время между последовательными опросами доступности
Retries (Повторные попытки подключения)	От 0 до 10 повторов По умолчанию: 3	Количество повторных опросов подключения, которые необходимо выполнить при сбое первоначального опроса
Timeout (Перерыв между повторными подключениями)	от 10 до 10000 мс По умолчанию: 700 мс	Количество времени, необходимое для ожидания ответа на опрос, прежде чем истечет время ожидания первого запроса на опрос. Значение тайм-аута удваивается при каждой последующей повторной попытке. Для тайм-аута = 700 мс (0,7 с) и повторных попыток = 3: - 0,7 с на первую повторную попытку - 1,4 с на повторную попытку - 2,8 с на третью попытку

Архитектура SNMP. Компоненты составляющие архитектуру (рисунок 1):

- сетевая станция управления, включающая в себя сетевого менеджера;
- агенты;
- мастер-агенты;
- управляемые компоненты.

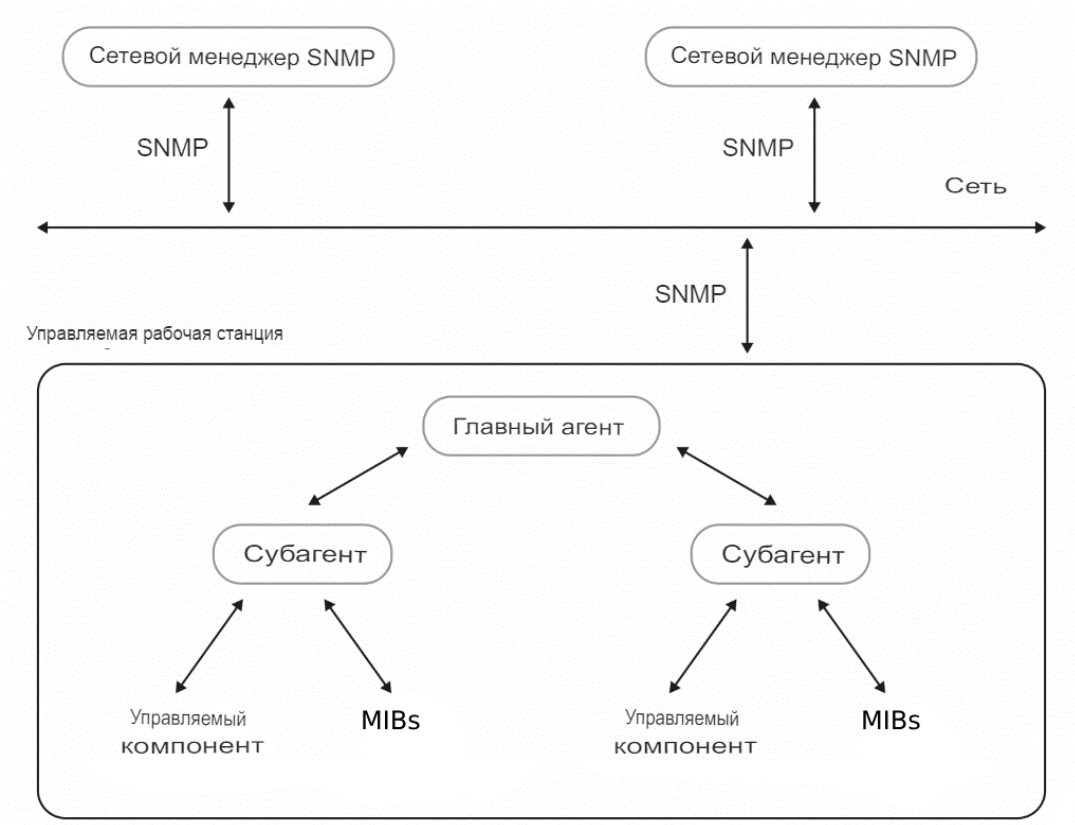

Рисунок 1. – Архитектура SNMP [2]

Агенты SNMP:

Мастер-агент – программа, связывающая сетевых менеджеров и субагентов. Мастер-агент анализирует запросы сетевого менеджера и пересылает их субагентам, собирает и формирует ответы субагентов и отправляет их менеджеру. Мастер-агент уведомляет менеджера, если запрос некорректен или запрошенная информация недоступна.

Субагент – программа, поставляемая вендором вместе с сетевым устройством. Субагент пересылает собранную информацию мастер-агенту. У каждого управляемого компонента есть соответствующий субагент.

Управляемый компонент – это подключенное к сети устройство или программное обеспечение с встроенным субагентом. К таким устройствам относятся не только маршрутизаторы, коммутаторы и серверы, но и IP-телефоны.

База управляющей информации (MIB) – иерархическая база данных со сведениями об оборудовании. У каждого типа устройства своя MIB-таблица, например, у коммутатора в ней содержится информация о трафике. Благодаря MIB менеджер знает, какую информацию он может запросить у агента устройства.

Коммуникация SNMP. В протоколе для общения между агентами и менеджерами используются ловушки (Trap). Это важнейший способ коммуникации в SNMP. Менеджер отвечает за большое количество устройств, на многих из них может быть несколько управляемых компонентов. Агент отправляет ловушку по своей инициативе, когда необходимо сообщить менеджеру о событии.

Получив уведомление, менеджер выбирает нужное действие, например, опрашивает агента, чтобы получить полное представление о том, что произошло. Перечень уведомлений, которые посылает ловушка:

- 0 – coldStart – холодный запуск устройства;
- 1 – warmStart – горячий запуск устройства;
- 2 – linkDown – интерфейс отключился;
- 3 – linkUp — Интерфейс включился;
- 4 – authenticationFailure — менеджер выслал сообщение с неверной строкой сообщества;
- 5 – egpNeighborLoss – агент потерял связь с хостом;
- 6 – entrpriseSpecific – произошло событие, характерное для производителя данного устройства.

В SNMP есть два типа ловушек: Trap и Inform. Отличия между ними в том, что после получения Inform менеджер подтверждает получение ловушки. В противном случае агент будет отправлять Inform, пока не получит подтверждения. А вот после получения Trap менеджер не отправляет подтверждение. Если сообщение не дошло до менеджера, агент об этом не узнает.

Безопасность SNMP-протокола. В зависимости от версии протокола, меняются модели его безопасности. Так в первой и второй версии протокола используется модель безопасности на основе строки сообщества. Фактически это идентификатор пользователя или пароль, который отправляется вместе с запросом. Если строка сообщества неверна, агент игнорирует запрос. Строки сообщества бывают трех видов:

- только для чтения – позволяет получать данные с устройства;
- чтение/запись – позволяет получать данные и изменять конфигурацию устройства;
- строка сообщества SNMP Trap – позволяет получать ловушки.

Строка сообщества широко используется из-за своей простоты и наличия внешних систем безопасности.

В третьей версии протокола используется модель, ориентированная на пользователя, благодаря которой стало возможным добавление модулей аутентификации и шифрования без смены базовой архитектуры. Предусмотрено 3 уровня безопасности:

- noAuthNoPriv – пароли передаются в открытом виде, конфиденциальность данных отсутствует;
- authNoPriv – аутентификация без конфиденциальности. Большинство пользователей использует именно этот уровень, так как уровень защищенности в нем уже достаточно высок, а сетевые устройства не перегружаются шифрованием данных;
- authPriv – аутентификация и шифрование. Данный уровень имеет максимальную защищенность.

Вывод. Основным преимуществом SNMP является простота и удобство настройки. С его помощью можно отслеживать все необходимые данные для настройки и мониторинга IP-телефонии.

ЛИТЕРАТУРА

1. How to use SNMP to monitor your VoIP network [Электронный ресурс]. – 2020. – Режим доступа: https://info.teledynamics.com/blog/how-to-use-snmp-to-monitor-your-voip-network. – Дата доступа: 05.10.2023.
2. Протокол управления SNMP [Электронный ресурс]. – 2021. – Режим доступа: https:// https://selectel.ru/blog/snmp/. – Дата доступа: 05.10.2023.
3. Кевин Дж. Основы SNMP/ Кевин Дж., Шмидт Дуглас, Р. Мауро; – 2-е изд. – Символ-Плюс , 2012.- 520 с.