УДК 004.724

Голубничая Е.Ю.,
кандидат технических наук, доцент
доцент кафедры «Сети и системы связи»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Каминский Р.В.,
студент
2 курс, факультет «Оптические и квантовые коммуникации»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ SNMP- И ICMP-МОНИТОРИНГА В СИСТЕМЕ ZABBIX

Аннотация: *статья посвящена подробному практическому исследованию возможностей сетевых протоколов ICMP и SNMP при использовании системы мониторинга Zabbix. Основной целью исследования является сравнительный анализ информативности данных методов мониторинга при наблюдении за состоянием серверной инфраструктуры. Экспериментальная часть реализована на виртуальном стенде, развернутом в среде VirtualBox. Стенд включает сервер мониторинга Zabbix, целевую виртуальную машину с установленным веб-сервером Apache, SNMP-агентом и системой управления базами данных PostgreSQL. На виртуальных машинах установлена РЕД ОС - современная операционная система российского производства на базе Linux.*

Ключевые слова: *мониторинг сетей, информационные системы, системное администрирование, сетевые протоколы, SNMP, ICMP, Zabbix мониторинг.*

Abstract: *This article is devoted to a detailed practical study of the capabilities of the ICMP and SNMP network protocols when using the Zabbix monitoring system. The primary objective of the study is to comparatively analyze the information content of these monitoring methods when monitoring the state of a server infrastructure. The experimental portion was implemented on a virtual rig deployed in a VirtualBox environment. The rig includes a Zabbix monitoring server, a target virtual machine with an Apache web server, an SNMP agent, and a PostgreSQL database management system installed. The virtual machines are running RED OS, a modern Russian-made Linux-based operating system.*

Keywords: *network monitoring, information systems, system administration, network protocols, SNMP, ICMP, Zabbix monitoring.*

Современные информационные системы характеризуются высокой степенью распределённости и сложной архитектурой, включающей множество серверов, сетевых устройств и прикладных сервисов. В таких условиях обеспечение стабильной работы инфраструктуры невозможно без использования специализированных систем мониторинга.

Одним из наиболее распространенных решений в данной области является система Zabbix, позволяющая осуществлять централизованный контроль состояния серверов, сетевых устройств и приложений в режиме реального времени. Основой мониторинга в подобных системах выступают различные протоколы сбора информации, среди которых наиболее простым и широко используемым является ICMP.

ICMP-мониторинг основан на отправке echo-запросов (ping) к целевому узлу и анализе ответов. Данный метод позволяет определить доступность хоста и базовые сетевые параметры, такие как задержка (latency) и потеря пакетов (packet loss). Однако ICMP не предоставляет информации о

внутреннем состоянии системы, что существенно ограничивает его применение в задачах глубокого анализа производительности.

В отличие от ICMP, протокол SNMP (Simple Network Management Protocol) обеспечивает доступ к расширенному набору системных и сетевых метрик, включая загрузку процессора, использование памяти, загрузку сетевых интерфейсов и другие параметры. Это делает SNMP более мощным инструментом для комплексного мониторинга инфраструктуры.

Актуальность исследования обусловлена необходимостью выбора оптимальных методов мониторинга в зависимости от задач администрирования, масштабов сетевой инфраструктуры и необходимого уровня детализации данных.

Для проведения исследования был развёрнут лабораторный стенд на базе виртуальной среды VirtualBox. Были созданы две виртуальные машины, на каждую из которых была установлена операционная система РЕД ОС. Такой подход позволил безопасно моделировать реальные условия сетевой инфраструктуры без существенного влияния на продуктивные системы.

Первая виртуальная машина (VM1) являлась сервером мониторинга. На ней был установлен и настроен Zabbix-server, обеспечивающий централизованный сбор метрик, обработку событий и управление триггерами, создана и настроена база данных PostgreSQL, без которой работа Zabbix не представляется возможной, т.к. PostgreSQL отвечает за хранение исторических данных мониторинга. Также были добавлены необходимые узлы сети для осуществления исследования.

Вторая виртуальная машина (VM2) являлась целевым сервером. Данный сервер использовался как объект мониторинга. Он являлся имитацией настоящего серверного узла в сети.

На целевой сервер был установлен SNMP-агент, (net-snmp), обеспечивающий предоставление системных и сетевых метрик для системы мониторинга Zabbix. Через SNMP осуществляется сбор информации о состоянии процессора, оперативной памяти, сетевых интерфейсов, а также

общей системной нагрузки. Это позволяет получать расширенную картину состояния сервера в реальном времени.

Для ICMP-мониторинга и проверки сетевой доступности использовалась утилита fping, которая была заранее предустановлена и применялась для выполнения пакетных ping-запросов и оценки стабильности сетевого соединения.

Также на целевом сервере был развернут веб-сервер Apache HTTP Server, который выполняет роль тестового веб-сервиса и используется для моделирования пользовательской нагрузки. Данный сервис позволяет анализировать поведение системы при увеличении количества HTTP-запросов и оценивать влияние нагрузки на системные ресурсы.

Для обеспечения взаимодействия между виртуальными машинами в лабораторном стенде был выбран режим сетевого моста (Bridged Adapter), что позволило интегрировать обе ВМ в единую локальную сеть. Также на каждой виртуальной машине были настроены статические IP-адреса, что обеспечило постоянную адресацию узлов и стабильную сетевую связность в процессе выполнения экспериментов и настройки мониторинга. Статические IP-адреса были назначены вручную с использованием настроек сетевого интерфейса и маршрутизатора.

В рамках исследования ICMP-мониторинг был реализован с использованием встроенных возможностей Zabbix без установки дополнительных агентов на целевой машине. Проверка доступности выполнялась посредством отправки ICMP Echo Request к узлу VM2 с использованием механизма fping.

Хост был добавлен в систему Zabbix с указанием IP-адреса целевого сервера, после чего активированы стандартные элементы мониторинга ICMP, включающие проверку доступности, измерение задержки ответа и анализ потерь пакетов. Получаемые данные позволяли оценивать общее состояние сетевого соединения между сервером мониторинга и целевым узлом. Иллюстрация ICMP-мониторинга приведена на рисунке 1.

Рисунок 1. ICMP-мониторинг целевого сервера, где верхний график отображает ICMP ping, нижний график – ICMP response time

В ходе эксплуатации установлено, что ICMP-мониторинг корректно фиксирует доступность узла.

Для расширения возможностей мониторинга и получения детализированной информации о состоянии целевого узла был использован протокол SNMP. В отличие от ICMP, данный протокол позволяет получать системные и сетевые метрики, отражающие внутреннее состояние операционной системы.

На целевом сервере был установлен и настроен SNMP-агент (net-snmp), обеспечивающий взаимодействие с системой мониторинга. В рамках лабораторной конфигурации использовалась упрощённая схема доступа с применением community-строки, что позволило обеспечить обмен данными между Zabbix Server и целевым узлом.

Корректность работы SNMP-агента была проверена с использованием утилиты snmpwalk, с помощью которой осуществлялся запрос дерева доступных параметров. Успешный ответ подтвердил доступность SNMP-интерфейса и корректность его настройки.

После этого хост был добавлен в систему Zabbix с указанием SNMP-интерфейса и применением стандартного шаблона мониторинга. В рамках SNMP-мониторинга осуществлялся сбор таких параметров, как загрузка процессора, использование оперативной памяти, состояние сетевых интерфейсов. Иллюстрации SNMP-мониторинга приведены на рисунках 2 и 3.

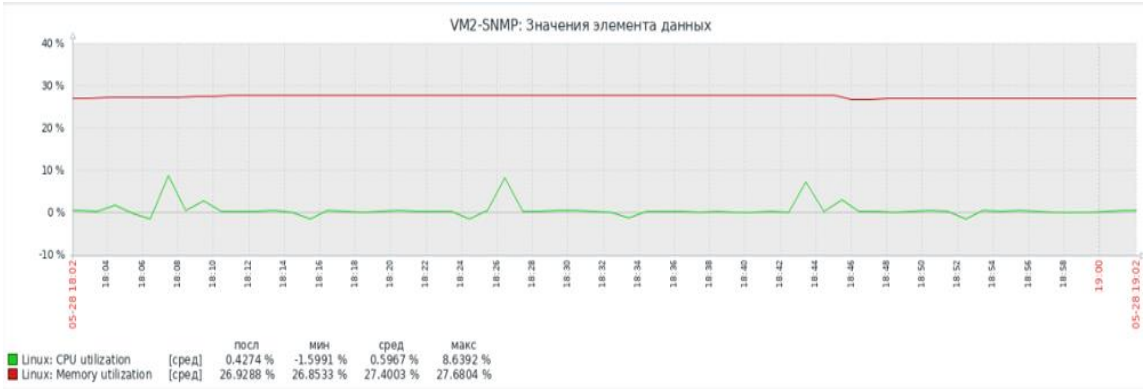

Рисунок 2. SNMP-мониторинг целевого сервера, где верхний график отображает memory utilization, нижний – CPU utilization

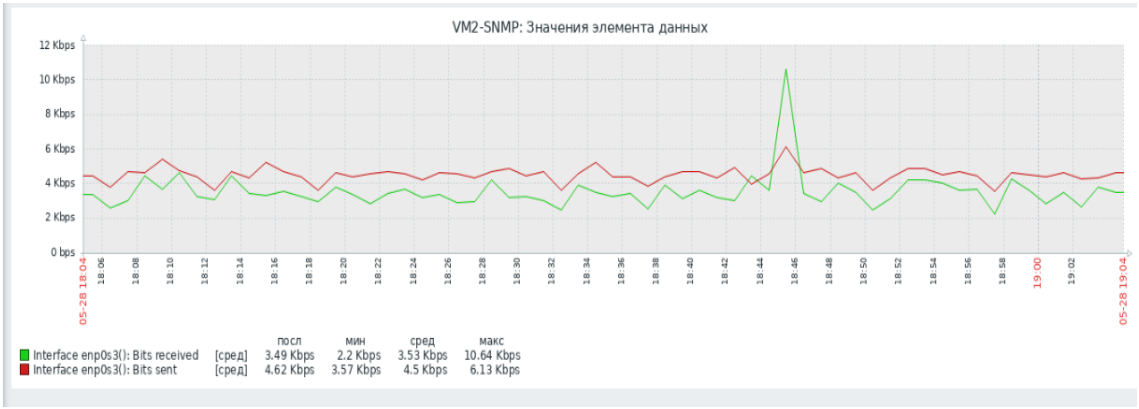

Рисунок 3. SNMP-мониторинг целевого сервера, отображающий передачу и приём сетевого трафика

Полученные результаты подтверждают корректную работу SNMP-мониторинга и успешную интеграцию SNMP-агента с системой Zabbix. В процессе наблюдения обеспечивался стабильный сбор системных метрик в режиме реального времени, включая загрузку процессора, использование оперативной памяти, сетевую активность и показатель системной нагрузки (load average). Это позволяет сделать вывод о корректной настройке SNMP-интерфейса и его готовности к использованию в рамках дальнейшего нагрузочного тестирования и сравнительного анализа с ICMP-мониторингом.

Нагрузочное тестирование и анализ поведения системы

Для оценки поведения системы мониторинга при повышенной нагрузке на веб-сервис было проведено нагрузочное тестирование целевого узла. Основной целью данного этапа являлось исследование изменений сетевых и системных параметров, фиксируемых средствами ICMP и SNMP, а также оценка устойчивости сервера Apache HTTP Server в условиях интенсивной обработки запросов.

Перед началом генерации нагрузки требовалось проверить статус работы Apache HTTP Server. Данное действие было выполнено командой systemctl status httpd, результаты которой проиллюстрированы на рисунке 4.

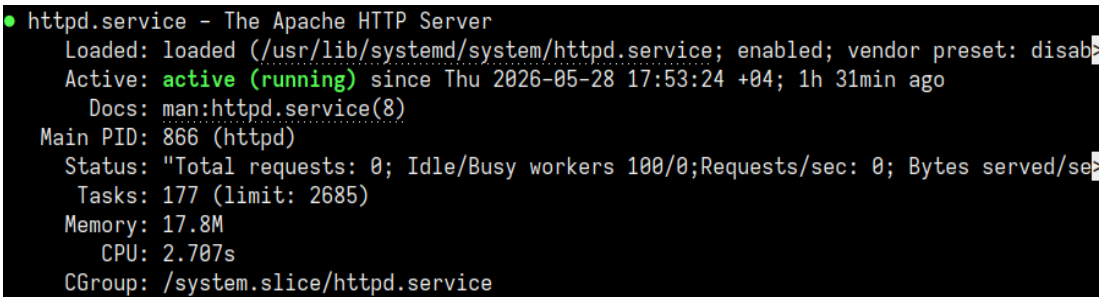

Рисунок 4. Проверка статуса работы Apache HTTP Server

Генерация нагрузки осуществлялась с использованием утилиты Apache Benchmark (ab), предназначенной для стресс-тестирования веб-серверов. В рамках эксперимента выполнялась отправка фиксированного количества HTTP-запросов с заданным уровнем параллелизма, что позволяло моделировать одновременную работу множества клиентов. Данный подход обеспечивал создание контролируемой нагрузки на веб-сервер Apache HTTP Server и позволял оценить поведение системы в условиях высокой интенсивности запросов. Ход работы утилиты проиллюстрирован на рисунке 5.

```
[root@localhost Kennyy]# ab -n 100000 -c 50 http://192.168.0.112/
This is ApacheBench, Version 2.3 <$Revision: 1913912 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 192.168.0.112 (be patient)
Completed 10000 requests
Completed 20000 requests
Completed 30000 requests
Completed 40000 requests
Completed 50000 requests
Completed 60000 requests
Completed 70000 requests
Completed 80000 requests
Completed 90000 requests
Completed 100000 requests
Finished 100000 requests
```

Рисунок 5. Успешно выполненная нагрузка на целевой сервер

В процессе тестирования осуществлялся одновременный мониторинг состояния целевого узла с использованием двух подходов: ICMP и SNMP. ICMP-мониторинг фиксировал доступность узла и параметры сетевого отклика, включая задержку и потерю пакетов. При этом даже в условиях повышенной нагрузки сервер продолжал отвечать на ICMP-запросы, что свидетельствует о сохранении базовой сетевой доступности. Результаты ICMP-мониторинга под искусственной нагрузкой приведены на рисунке 6.

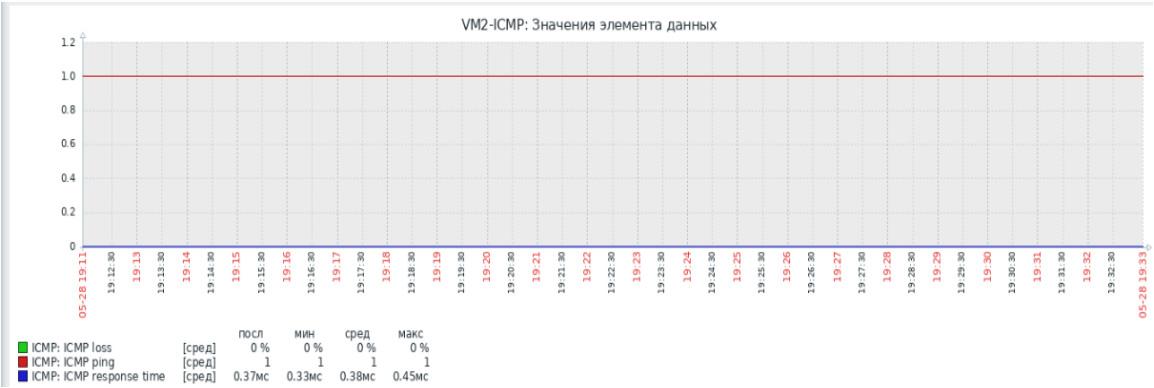

Рисунок 6. ICMP-мониторинг целевого сервера (после генерации нагрузки), где верхний график отображает ICMP ping, нижний график – ICMP response time.

В то же время SNMP-мониторинг позволял наблюдать внутренние изменения состояния системы. В частности, фиксировался рост загрузки центрального процессора, увеличение использования оперативной памяти, а также повышение уровня сетевой активности. Иллюстрации показателей SNMP-мониторинга после генерации нагрузки приведены на рисунках 7 и 8.

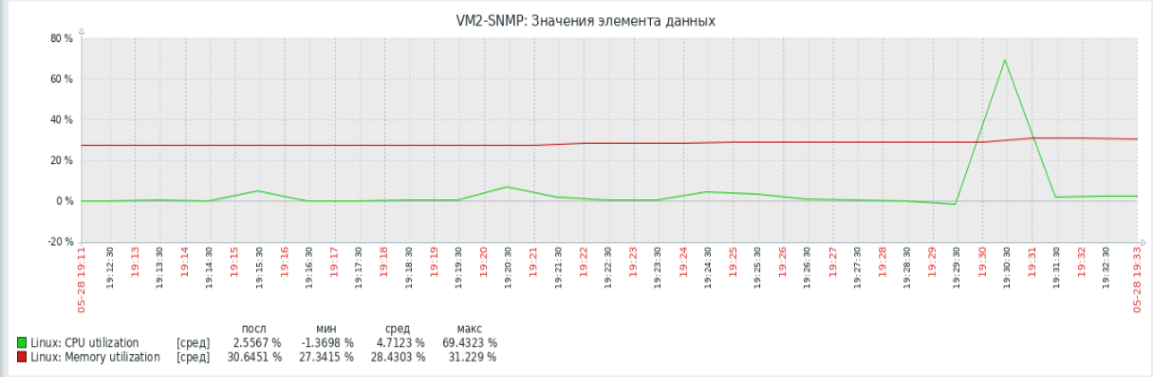

Рисунок 7. SNMP-мониторинг целевого сервера (после генерации нагрузки), где верхний график отображает memory utilization, нижний – CPU utilization

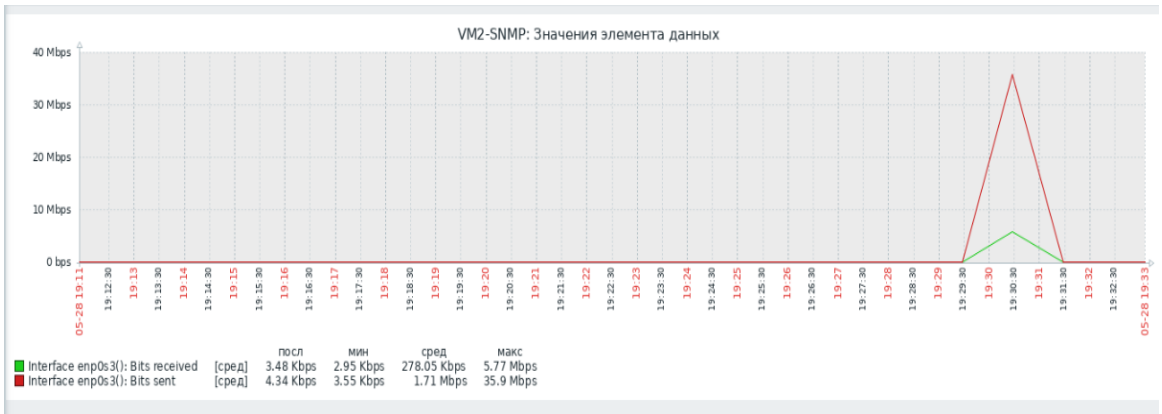

Рисунок 8. SNMP-мониторинг целевого сервера (после генерации нагрузки), отображающий передачу и приём сетевого трафика

Для более наглядного сравнения результатов ICMP- и SNMP-мониторинга в условиях отсутствия и наличия нагрузки были сведены основные количественные показатели, отражающие изменения сетевых и

системных параметров. Полученные значения позволяют провести сравнительный анализ эффективности обоих подходов к мониторингу.

Таблица 1.

Сравнение показателей ICMP- и SNMP-мониторинга до и после нагрузки

Протокол	**Метрика**	**До нагрузки**	**После нагрузки (пик/среднее)**	**Изменение**
ICMP	Потеря пакетов (loss)	0%	0%	-
ICMP	Время ответа (response time)	0.41 мс (среднее)	0.38 мс (среднее)	-7%
ICMP	Ping (TTL/порядок)	1	1	-
SNMP	CPU utilization	~0,5% (сред.)	Пик 69,4%	Более чем в 140 раз
SNMP	Memory utilization	~27% (стабильно)	Пик 31,2%	Увеличение на 4%.
SNMP	Network received (RX)	3,5 КБит/с (сред.)	Пик 35,9 Мбит/с	Больше приблизительно в 10000 раз
SNMP	Network sent (TX)	4.6 КБит/с (сред.)	Пик 5,8 Мбит/с	Больше приблизительно в 1200 раз

В результате проведённого исследования и нагрузочного тестирования установлено, что ICMP-мониторинг обеспечивает лишь базовый контроль доступности сетевых узлов и сохраняет работоспособность даже при значительной нагрузке на сервер, не отражая при этом изменений внутренних

ресурсов системы. SNMP-мониторинг, в свою очередь, позволяет фиксировать изменения ключевых системных параметров, включая загрузку процессора, использование оперативной памяти и сетевую активность, что обеспечивает более глубокий и информативный анализ состояния серверной инфраструктуры. Таким образом, результаты исследования подтверждают, что полноценный мониторинг сетевой инфраструктуры требует использования SNMP, поскольку ICMP не обеспечивает достаточного уровня детализации данных о состоянии узлов.

Использованные источники:

1. Zabbix Documentation. Official Zabbix Manual [Электронный ресурс]. URL: https://www.zabbix.com/documentation/ (дата обращения: 27.05.2026).
2. Stallings, W. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2* / W. Stallings. — 3rd ed. — Boston: Addison-Wesley, 1999. — 640 p.
3. Kurose, J. F., Ross, K. W. *Computer Networking: A Top-Down Approach*. — 8th ed. — Pearson, 2021. — 864 p.
4. Nemeth, E., Snyder, G., Hein, T. *UNIX and Linux System Administration Handbook*. — 5th ed. — Pearson, 2017. — 1200 p.
5. Apache HTTP Server Documentation. Official Apache Docs [Электронный ресурс]. URL: https://httpd.apache.org/docs/ (дата обращения: 28.05.2026).
6. Net-SNMP Project Documentation [Электронный ресурс]. URL: https://www.net-snmp.org/docs/ (дата обращения: 28.05.2026).
7. ICMP Protocol Specification (RFC 792) [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc792 (дата обращения: 28.05.2026).
8. PostgreSQL Documentation [Электронный ресурс]. URL: https://www.postgresql.org/docs/ (дата обращения: 28.05.2026).