УДК 004.771

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ СЕТЕВОГО МОНИТОРИНГА С ПРИМЕНЕНИЕМ ПРОТОКОЛА ICMP

Голубничая Е.Ю.

к.т.н., доцент

Самарский государственный технический университет,

Самара, Россия

Аннотация

В работе рассматриваются особенности практической реализации мониторинга доступности хостов с применением протокола ICMP, в том числе с использованием специализированного программного обеспечения «10-Страйк: Мониторинг Сети». Для анализа трафика применяется сниффер Wireshark, который позволяет наглядно отследить входящий и исходящий трафик, в том числе трафик протокола ICMP. В исследуемом сценарии производился мониторинг сайта университета (https://lk.samgtu.ru), в процессе которого от хоста с которого осуществлялся мониторинг (клиент) в автоматизированном режиме с заданной периодичностью отправлялись ICMP-запросы на IP-адрес сайта (сервер), с которого затем поступали ICMP-ответы. В процессе мониторинга доступности сервера сайта выполнен анализ времени отклика сервера.

Ключевые слова: хост, мониторинг сети, эхо-запрос, эхо-ответ, ping, ICMP, Wireshark.

PECULIARITIES OF PRACTICAL REALIZATION OF NETWORK MONITORING WITH THE USE OF ICMP PROTOCOL

Golubnichaya E.Yu.

Candidate of Technical Sciences (PhD Eng.), Associate Professor

Samara State Technical University,

Samara, Russia

Abstract

The paper deals with the peculiarities of practical implementation of host availability monitoring using ICMP protocol, including the use of specialized software «10-Strike: Network Monitoring». Wireshark sniffer is used for traffic analysis, which allows to visually track incoming and outgoing traffic, including ICMP protocol traffic. In the scenario under study, the university website (https://lk.samgtu.ru) was monitored, in the course of which ICMP-requests were sent from the host from which the monitoring was performed (client) to the IP-address of the website (server) in the automated mode with a specified periodicity, from which ICMP-replies were then received. In the process of monitoring the availability of the site server, the server response time was analyzed.

Keywords: host, network monitoring, echo request, echo reply, ping, ICMP, Wireshark.

В настоящее время наряду со стремительным проникновением в жизнь современного общества информационных технологий возрастает и необходимость своевременного доступа к ресурсам сети с должным уровнем качества обслуживания. К примеру, отсутствие доступа к сайту в нужный момент времени может доставить пользователю определенные неудобства, а в некоторых случаях и явиться серьезной проблемой. Так, например, если абонент решил в последний момент времени передать показания счетчиков электроэнергии через сайт в нерабочее время специалистов абонентского отдела, то при отсутствии доступа к сайту он не сможет этого сделать. Примерно такая же ситуация возникнет если рассмотреть случай отсутствия у студента доступа в личный кабинет на сайте университета ввиду технических проблем на сервере, что может привести к тому, что студент не сможет загрузить свои работы (отчеты по лабораторным и практическим занятиям) в

установленные временные рамки.

Ввиду вышеизложенного становится вполне очевидным то, что системным администраторам необходимо выполнять непрерывный мониторинг доступности сетевых ресурсов и в случае возникновения (обнаружения) технических проблем оперативно устранять их до обнаружения проблем конечными пользователями. Безусловно, в наш век высоких технологий мониторинг сети производится с использованием специализированных программных продуктов в автоматизированном режиме, позволяющих производить мониторинг в удаленном режиме [1], в том числе с использованием протокола ICMP (Internet Control Message Protocol) [2, 3].

Протокол межсетевых управляющих сообщений ICMP позволяет осуществлять мониторинг доступности хостов посредством отправки эхо-запросов (тип 8) по соответствующему IP-адресу анализируемого хоста и получении соответствующих эхо-ответов (тип 0) на данные запросы. То есть простыми словами принцип работы ICMP можно объяснить на примере, когда человек стучится в чужую дверь, если после стука ему открыли дверь, то это означает, что доступ для дальнейшего взаимодействия у него есть, если же дверь не открывается, тогда доступа нет и нужно искать пути решения возникшей проблемы. Применение протокола ICMP для мониторинга хостов в глобальной сети возможно с использованием сети Интернет, а в локальной сети с использованием сети Ethernet.

В случае если на все отправленные эхо-запросы ICMP были получены эхо-ответы, то можно судить от стабильной доступности анализируемого хоста. Если же часть эхо-запросов, остается без ответа от анализируемого хоста, тогда системному администратору необходимо оперативно выявить дестабилизирующие факторы, которые являются причиной нестабильного соединения. Если же от анализируемого хоста совсем не поступают ответы, тогда связь с сервером отсутствует и системному администратору необходимо оперативно выявить и решить возникшие проблемы. Необходимо обратить

внимание на то, что в настоящей работе речь идет именно о легитимном мониторинге, то есть когда на стороне анализируемого хоста не установлены запреты на входящий и исходящий трафик (в т.ч. ICMP) от соответствующего хоста с которого осуществляется мониторинг [4].

Мониторинг доступности хостов может осуществляться с использованием возможностей командной строки операционной системы и встроенной утилиты *ping*. Причем при использовании утилиты *ping* совсем необязательно в синтаксисе команды указывать IP-адрес анализируемого хоста, можно указать доменное имя сайта. На рис. 1 представлен внешний вид окна командной строки, где наглядно видно, что по результатам выполнения команды «*nslookup lk.samgtu.ru*» был определен IP-адреса сервера данного сайта «*194.190.143.44*», который также был определен и при выполнении команды *ping* с указанием доменного имени данного сайта.

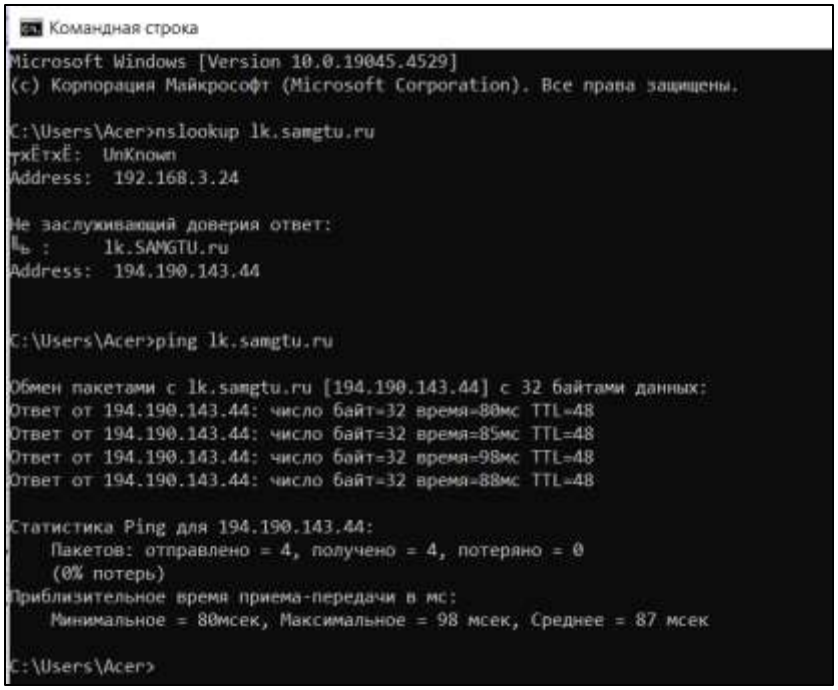

Рис. 1. Проверка доступности хоста с использованием утилиты ping

На рис. 2 представлены результаты по захвату трафика снифферо Wireshark с применением фильтра «icmp» в процессе выполнения команды

ping.

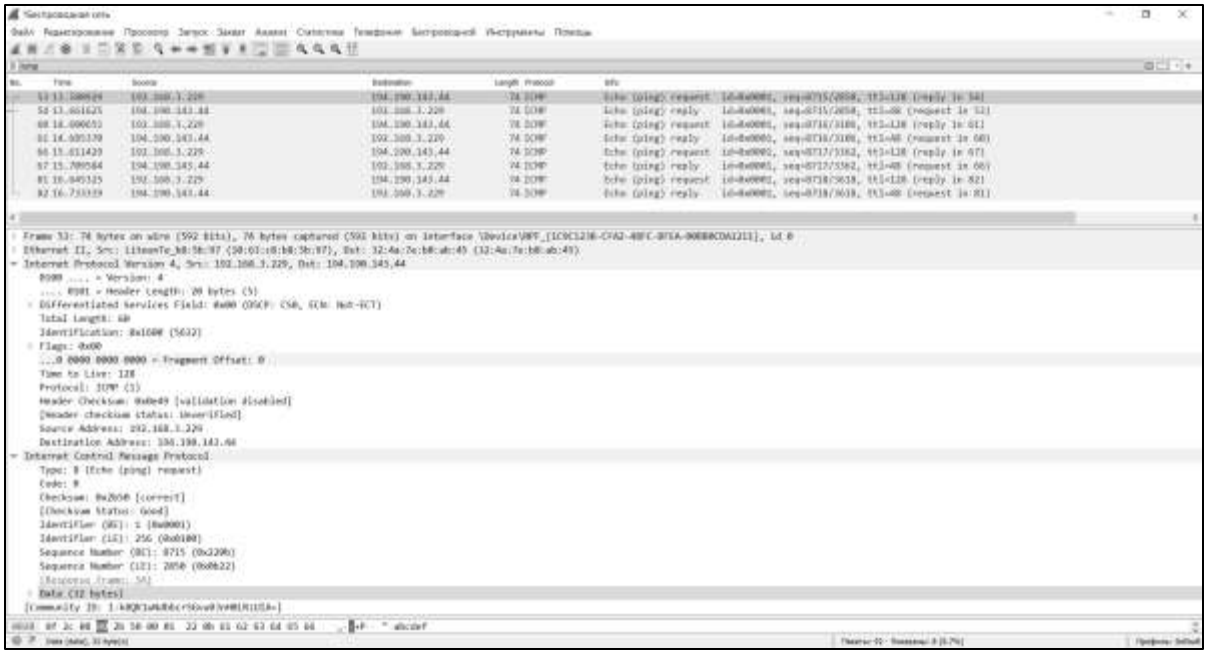

Рис. 2. Захват трафика ICMP сниффером Wireshark при использовании утилиты ping

Анализируя, представленные на рис. 1 и рис. 2 результаты, с целью проверки доступности сайта, команды «*ping lk.samgtu.ru*», можно наглядно увидеть, что на все 4 отправленных эхо-запроса были получены эхо-ответы. При этом минимальное время отклика между парой «запрос-ответ» составило 80 мс, максимальное – 98 мс, среднее – 87 мс. Значение времени отклика зависит от многих причин, как на стороне исходного хоста, так и анализируемого хоста. К примеру, время отклика хоста может увеличиваться в случае загрузки сети на стороне исходного/входящего хоста или при увеличении размера ICMP-запроса.

Сниффер Wireshark позволяет производить детальный анализ пакетного трафика, так на рис. 2 в пакете №53 наглядно виден IP-адрес отправителя «192.168.3.229» запроса и получателя запроса «194.190.143.44». Отправителем ICMP-запроса является персональный компьютер пользователя (системный администратор), при этом для доступа в сеть Интернет используется адаптер

беспроводной сети, характеристики которого представлены на рис. 3.

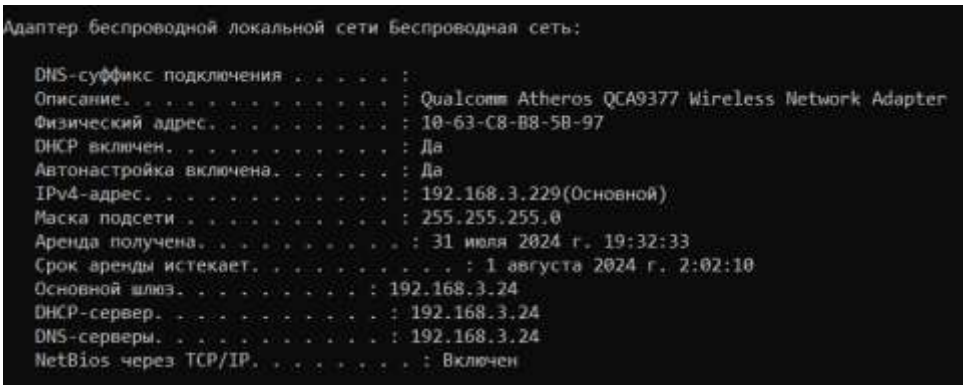

Рис. 3. Параметры адаптера беспроводной сети

Анализируя рис. 2 и рис. 3 видно, что Wireshark в захваченном трафике отображает не только IP-адреса, но и MAC-адреса устройств. Так, MAC-адрес (физический адрес) устройства, отправившего ICMP-запрос «10-63-C8-B8-5B-97» (раздел «Ethernet II» в отправленном пакете №53 «*Src: LiteonTe_b8:5b:97 (10:63:c8:b8:5b:97)*»). Аналогичная информация представлена и по устройству получившему эхо-запрос ICMP и в последствие отправившем эхо-ответ ICMP (раздел «Ethernet II» в отправленном пакете №53 «*Dst: 32:4a:7e:b0:ab:45*»). Пара «запрос-ответ» ICMP связаны между собой одинаковыми последовательными номерами (Sequence Number (BE), Sequence Number (LE)), к примеру, на рис. 2 наглядно видно, что пакет №53 и пакет №54 имеют одинаковые идентификаторы (*seq=8715/2850*).

Необходимо обратить внимание на то, что на рис. 1 представлен результат выполнения команды ping без указания дополнительных параметров в синтаксисе команды, поэтому была выполнена стандартная команда *ping*, включающая 4 запроса с полезными данными размером 32 байт. Однако при выполнении команды *ping* можно задать уточняющие параметры, тем самым задав, например, конкретное число отправляемых запросов проверки связи (параметр «-n <число>»), размер полезных данных в пакете (параметр «-l <размер>») и т.д. (рис. 4). Однако даже при задании в синтаксисе команды ping

параметра «-t», то есть по сути запуска непрерывного мониторинга, администратору сети необходимо будет выполнять мониторинг вручную, поскольку в этом случае обнаружить проблему он сможет только самостоятельно, анализируя полученные результаты (анализ трафика и/или результатов в командной строке).

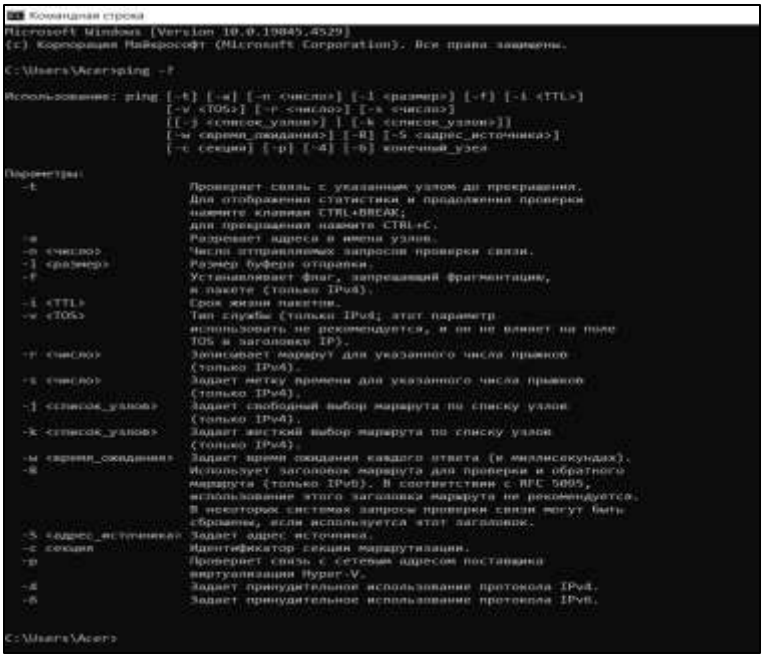

Рис. 4. Параметры утилиты ping

С учетом вышеизложенного становится очевидным, что для непрерывного мониторинга доступности хостов по протоколу ICMP и оперативного реагирования на возникшие проблемы, существует необходимость в применении специализированного программного обеспечения (ПО), посредством которого системный администратор сможет не только организовать удаленный мониторинг, но и оперативно узнать о проблеме, даже если он в настоящее время не находится у компьютера, с которого запущен мониторинг. В настоящее время существует довольно большое число программных продуктов, позволяющих реализовать автоматизированный мониторинг доступности хостов, в числе которых важное место занимают

Zabbix, Prometheus, «10-Страйк: Мониторинг Сети» и др. В текущей работе будет использоваться ПО «10-Страйк: Мониторинг Сети» в частности версия «Pro 7.6» с 31 дневным пробным (бесплатным) периодом [5]. Необходимо обратить внимание на то, что программы 10-Strike включены в единый реестр российских программ для ЭВМ Минцифры и могут участвовать в госзакупках.

В используемой версии ПО «10-Страйк: Мониторинг Сети» можно осуществлять мониторинг как хостов локальной сети, так и хостов в глобальной сети. На рис. 5 представлен скриншот интерфейса программы, на котором также отображен уже добавленный в мониторинг хост с IP-адресом 194.190.143.44, т.е. сайт «*lk.samgtu.ru*». Как видно на рис. 5 мониторинг выполняется успешно, время отклика сайта составляет 65 мс, что не превышает допустимое значение, поскольку установлен статус проверки «Успешно завершилась».

Рис. 5. Мониторинг доступности хоста с использованием ПО «10-Страйк: Мониторинг Сети»

Функциональные возможности ПО «10-Страйк: Мониторинг Сети»

(версия «Pro 7.6») позволяют настроить не только такие стандартные параметры мониторинга по ICMP как размер пакета, количество отправляемых эхо-запросов в одной проверке, интервалы между проверками, но и параметры автоматизированного мониторинга, такие как «Контроль времени выполнения» (рис. 6), что позволит установить максимальное допустимое время отклика для успешной проверки, при превышении которого администратору сети будет отправлено соответствующее оповещение в автоматизированном режиме [6].

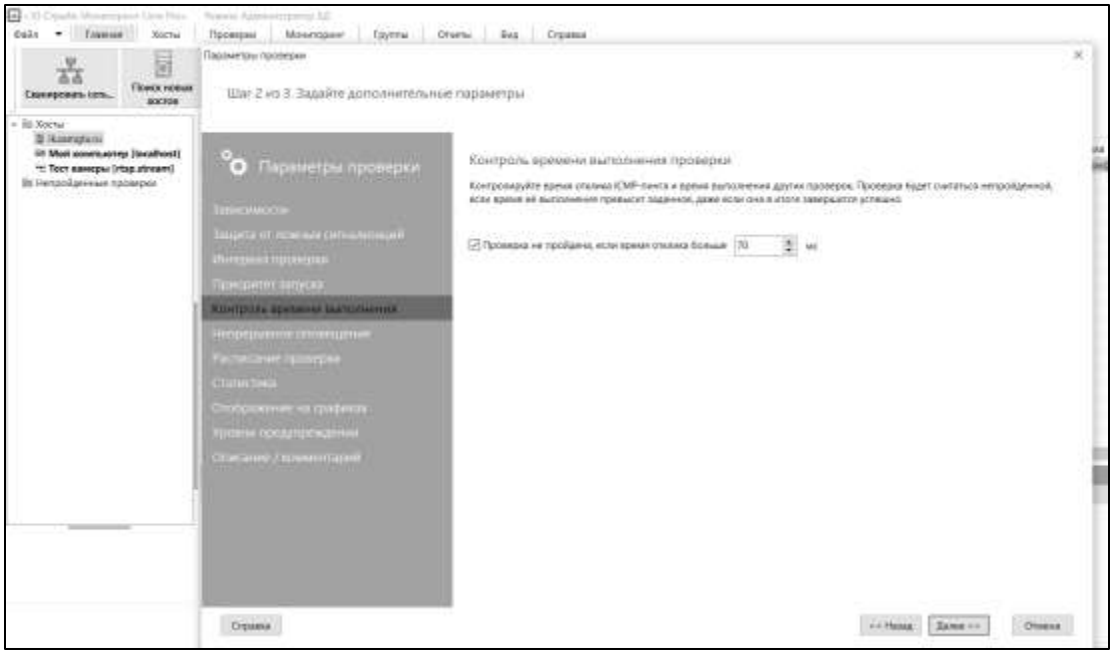

Рис. 6. Настройка предельного времени отклика для успешных проверок в ПО «10-Страйк: Мониторинг Сети»

Как видно на рис. 6 предельное время для успешных проверок установлено 70 мс, т.е. в случае если между парой «запрос-ответ» задержка превысит 70 мс, тогда ПО «10-Страйк: Мониторинг Сети» должно оповестить об этом системного администратора. При этом в целях защиты от ложных сигнализаций можно задать несколько попыток проверок после первой неудачной попытки перед оповещением (в рассматриваемом сценарии – 2 попытки с задержкой 30 мс). Необходимо обратить внимание на то, что по

времени отклика можно судить не только по пропускной способности между двумя хостами, но задав большое время отклика можно идентифицировать не отвеченные запросы. Каким образом будет происходить оповещение администратора, то есть задание действий, которые будут выполняться при соответствующих результатах проверки, определяет сам администратор, руководствуясь функциональными возможностями программы. В рассматриваемом сценарии, задано оповещение в виде сообщения на экран компьютера и сообщения на указанный e-mail (рис. 7). Кроме того задано звуковое оповещение на компьютере администратора.

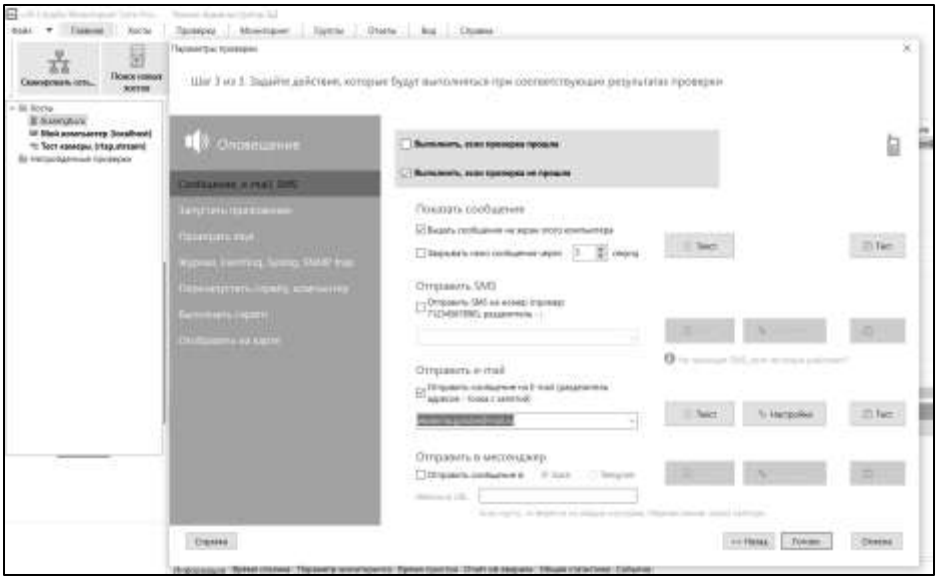

Рис. 7. Настройка действий при соответствующих результатах проверки в ПО «10-Страйк: Мониторинг Сети»

Для того чтобы оповещения приходили на заданный e-mail необходимо ввести необходимые данные по e-mail, с которого будут поступать соответствующие сообщения (рис. 8). В рассматриваемом сценарии сообщения будут отправляться с почты автора данной работы на эту же его почту, т.е. письмо себе.

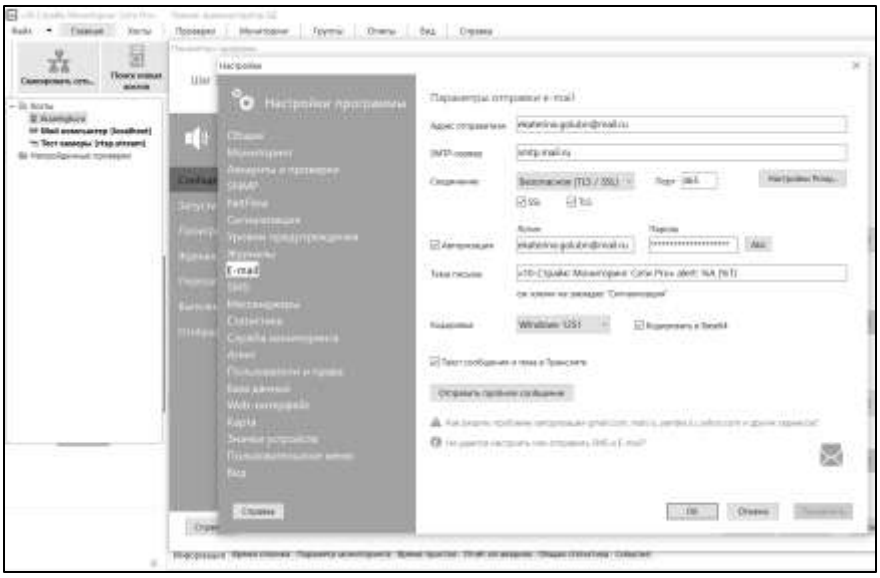

Рис. 8. Настройка параметров отправки оповещения на e-mail

Таким образом, при превышении допустимого времени отклика установленного в данном сценарии 70 мс (см. рис. 6) ПО «10-Страйк: Мониторинг Сети» должно автоматически оповестить администратора о возникшей проблеме, поскольку при заданных настройках данная проверка будет считаться неуспешной, что будет говорить о нестабильном соединении. На рис. 9 представлен скриншот, на котором наглядно видно, что при превышении времени отклика на 6 мс система выдала соответствующее текстовое оповещение на экран текущего компьютера, кроме того установлен новый статус проверки «Не прошла» и выдано звуковое оповещение. Аналогичное оповещение поступило на заданный e-mail (рис. 10).

Рис. 9. Оповещение на экране о превышении допустимого времени отклика

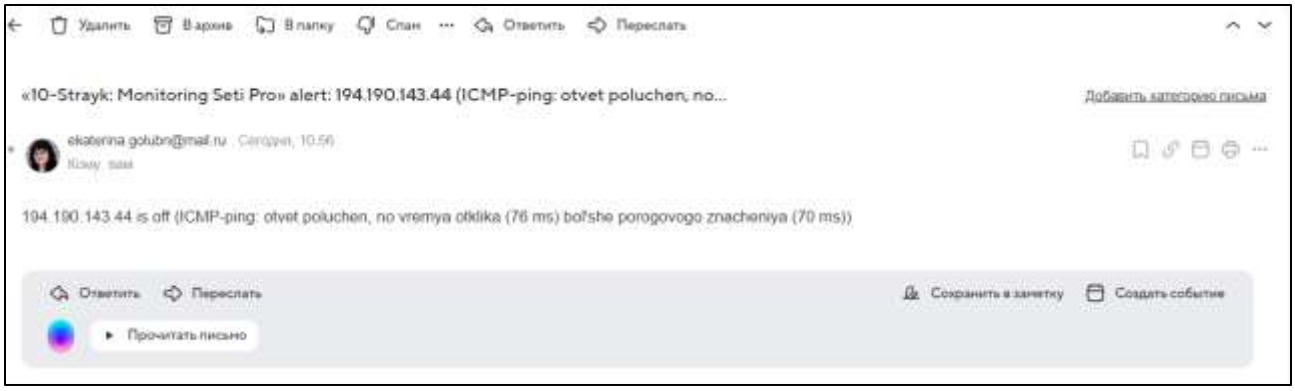

Рис. 10. Оповещение на e-mail о превышении допустимого времени отклика

Анализируя захваченный в рамках исследуемого сценария трафик ICMP по соответствующему фильтру «*ip.addr==194.190.143.44 && ip.addr==192.168.3.229 && icmp*», наглядно видно, что было захвачено всего 79340 пакетов, из которых 9676 пакетов ICMP. Такое большое количество пакетов объясняется именно непрерывным мониторингом (задано 100 запросов в одной проверке с интервалом между проверками – 60 с).

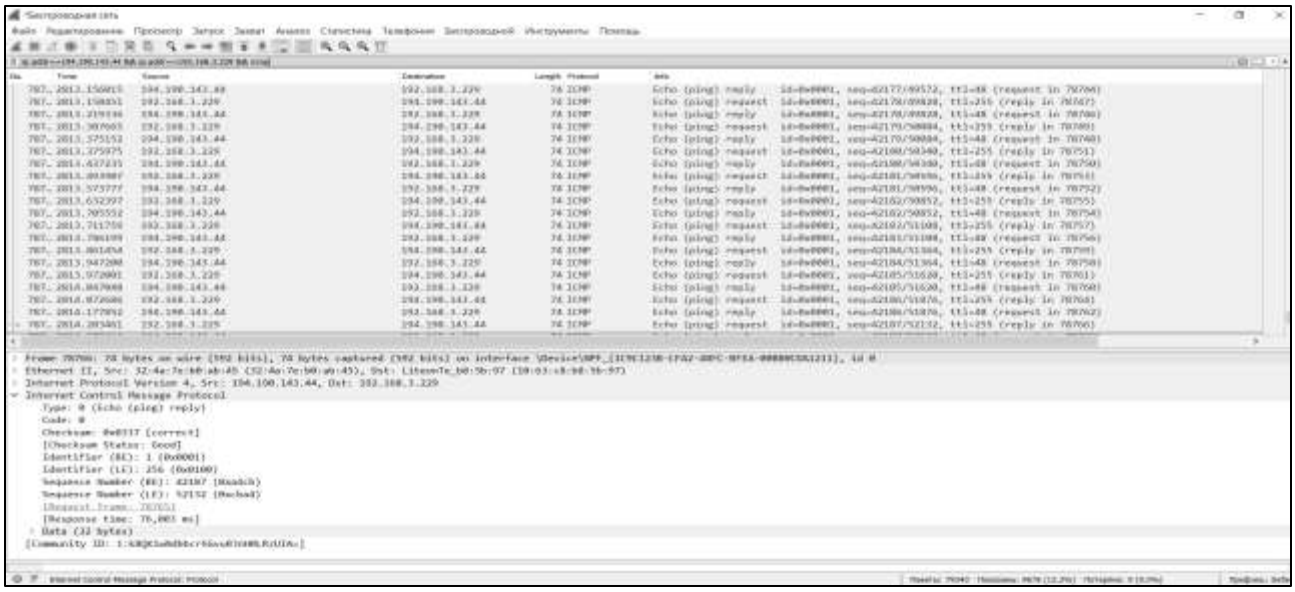

Рис. 11. Захват трафика ICMP сниффером Wireshark при использовании ПО «10-Страйк: Мониторинг Сети»

Таким образом, с учетом вышеизложенного можно сделать вывод о том, что применение протокола ICMP для мониторинга доступности хостов в настоящее время является актуальным. Однако для непрерывного автоматизированного мониторинга необходимо использовать специализированное ПО, которое позволит в случае возникновения проблем оповестить об этом системного администратора (e-mail, sms и т.д.).

Библиографический список

1. Добровольская Э.А. Отечественные системы мониторинга сети / Э.А. Добровольская // Современные информационные технологии: сборник научных статей по материалам 9-й Международной научно-технической конференции. – Бургас, 2023. – С. 108-114.

2. Голубничая Е.Ю. Мониторинг сети с использованием протокола ICMP / Е.Ю. Голубничая, Н.И. Денесюк // Системы синхронизации, формирования и обработки сигналов. – 2024. – Т. 15. – № 2. – С. 24-31.

3. Голубничая Е.Ю. Практическое применение автоматизированных систем сетевого мониторинга на базе протокола ICMP / Е. Ю. Голубничая, Н.И. Денесюк // Актуальные проблемы науки и техники: материалы II Международной научно-технической конференции, посвященной 70-летию ИМИ – ИжГТУ и 60-летию СПИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова». – Ижевск, 2022. – С. 730-734.

4. Голубничая Е.Ю. Фильтрация вредоносного трафика ICMP при обнаружении DDoS-атак // Е.Ю. Голубничая, В.Д. Зольников // Актуальные проблемы информатики, радиотехники и связи. Материалы XXXI Российской научно-технической конференции. – Самара, 2024. – С. 87-89.

5. Программа «10-Страйк Мониторинг Сети» – система мониторинга серверов и оборудования сети [Электронный ресурс]. – Режим доступа: https://www.10-strike.ru/network-monitor (Дата обращения 15.07.2024)

6. Князев Ю. «10-Страйк: мониторинг сети pro». Система мониторинга сети и оборудования / Ю. Князев // Системный администратор. – 2017. – № 9 (178). – С. 30-34.

Оригинальность 81%