ISSN 2079-8490

Электронное научное издание
«Ученые заметки ТОГУ»
2018, Том 9, № 1, С. 15 – 24

Свидетельство
Эл № ФС 77-39676 от 05.05.2010
http://pnu.edu.ru/ru/ejournal/about/
ejournal@pnu.edu.ru

УДК 338.2

© 2018 г. **А. С. Смирнов,**
Е. А. Шеленок, канд. техн. наук
(Тихоокеанский государственный университет, Хабаровск)

МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ КОМПЬЮТЕРА

В статье описаны сетевые протоколы для мониторинга сетевой активности компьютера. Представлены результаты работы программы для мониторинга сетевой активности.
Ключевые слова: протоколы, сеть, мониторинг, программная реализация.

A. S. Smirnov, E. A. Shelenok

MONITORING THE NETWORK ACTIVITY OF THE PERSONAL COMPUTER

The article describes network protocols for monitoring network activity of a computer. The results of the program for monitoring network activity are presented.
Keywords: protocols, network, monitoring, software implementation.

Введение

Компьютеры и компьютерные сети – важная часть сегодняшнего мира, а область их применения охватывает буквально все сферы человеческой деятельности. Последние два десятилетия характеризуются динамичным развитием сетевых технологий. Это связано с широкой популярностью, пришедшей к Интернету, развитием веб-технологий, электронной почты, потокового аудио и видео, систем обмена сообщениями в реальном времени.

Так как компьютерная сеть представляет собой сложную и дорогую систему, решающую ответственные задачи и обслуживающую большое количество пользователей, очень важно, чтобы сеть не просто работала, но работала качественно. Для этого существуют специальные программы для мониторинга.

Мониторинг в информационной структуре, будь то маленькая компания или огромный дата-центр, нужен, чтобы системные администраторы были оповещены о поломках и проблемах в инфраструктуре раньше или хотя бы одновременно с пользователями. Необходимость прогнозирования, а тем самым и предотвращения поломок, оповещения о них и хранения информации о состоянии систем очень важна.

В данной статье рассматриваются сетевые протоколы для мониторинга сетевой активности и разработанная программа для мониторинга сетевой активности компьютера.

Суть задачи мониторинга сетевой активности компьютера

Чтобы поддерживать любую сеть в рабочем состоянии и обеспечивать ее безопасность, необходимо вести постоянное наблюдение. Для этого существует такая задача, как мониторинг сетевой активности компьютера.

Мониторинг корпоративных сетей – критически важная функция ИТ, которая позволяет добиться экономии при повышении производительности инфраструктуры, высокой эффективности деятельности сотрудников, а также предоставляет возможность уменьшить затраты.

Сетевой мониторинг может выполняться с помощью различных программных средств или сочетания аппаратных устройств, функционирующих в режиме plug-and-play (включил и играй или работай), и программных решений. Можно осуществлять мониторинг практически любой сети – проводной или беспроводной, локальной сети предприятия, виртуальной частной сети или инфраструктуры, предоставляемой провайдером.

Мониторинг способен охватывать устройства с различными операционными системами и множеством функций – от сотовых телефонов до серверов, маршрутизаторов и коммутаторов.

Мониторинг помогает выявить любую специфическую активность в сети, определить параметры производительности и предоставить результаты, которые позволяют решать множество разнообразных задач, включая выполнение технических требований, предупреждение о внутренних угрозах безопасности и обеспечение прозрачности сетевых операций.

Сетевые протоколы для мониторинга сетевой активности

На транспортном уровне основными протоколами мониторинга и сбора статистики являются протоколы TCP и UDP.

TCP — один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных. TCP — это транспортный механизм, предоставляющий поток данных, с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета.

В отличие от UDP гарантирует целостность передаваемых данных и уведомление отправителя о результатах передачи.

Данные, которые можно получить для протокола TCP:

1) количество текущих подключений;
2) общее число установленных соединений;
3) количество пассивных соединений;
4) количество активных соединений;
5) количество сбоев при подключении;
6) количество сброшенных подключений;
7) получено сегментов;
8) отправлено сегментов;
9) повторно отправлено сегментов.

Среди набора протоколов Интернета есть транспортный протокол без установления соединения – UDP. Он позволяет посылать сообщения (в данном случае называемые датаграммами) другим компьютерам по IP-сети. UDP предоставляет ненадёжный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении.

Данные, которые можно получить для протокола UDP:

1) получено датаграмм;
2) отправлено датаграмм;
3) отсутствие портов;
4) ошибки при получении.

Другими, но менее значимыми протоколами для получения сетевой статистики являются протоколы ICMP и ARP.

ICMP в основном используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции. Утилита ping, служащая для проверки возможности доставки IP-пакетов использует ICMP-сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ).

Эхо-запрос и эхо-ответ, в совокупности, называемые эхо-протоколом, представляют собой очень простое средство мониторинга сети. Компьютер или маршрутизатор посылает по составной сети ICMP-сообщение эхо-запроса, указывая в нем IP-адрес узла, достижимость которого нужно проверить.

Узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса. Так как эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, то их

успешная доставка означает нормальное функционирование всей транспортной системы составной сети.

Утилита ping обычно посылает серию эхо-запросов к тестируемому узлу и предоставляет пользователю статистику об утерянных эхо-ответах и среднем времени реакции сети на запросы.

Пример работы утилиты ping представлен на рис. 1.

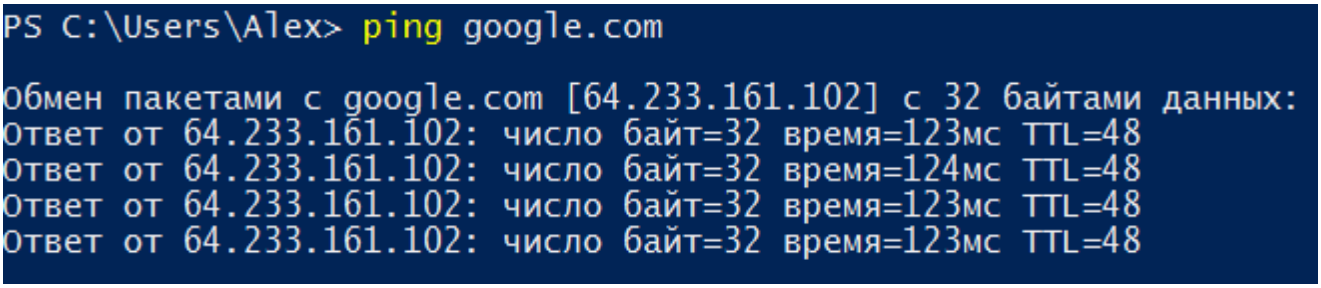

Рис. 1. Работа команды ping

Из приведенного рисунка видно, что в ответ на тестирующие запросы, посланные узлу google.com, было получено четыре эхо-ответа. Длина каждого сообщения составляет 32 байта. В следующей колонке помещены значения времени оборота, то есть времени от момента отправки запроса до получения ответа на этот запрос. Как видно, сеть работает стабильно. На экран выводится также оставшееся время жизни поступивших пакетов.

ARP – протокол канального уровня, предназначенный для определения MAC-адреса по известному IP-адресу.

Наибольшее распространение этот протокол получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку практически в 100% случаев при таком сочетании используется ARP.

Принцип работы:

1. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.

2. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным.

3. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Преобразование адресов выполняется путем поиска в таблице. Эта таблица, называемая ARP-таблицей, хранится в памяти и содержит строки для каждого узла сети.

В ARP-таблице для каждого IP-адреса содержит четыре кода:

1) Ifindex – Физический порт (интерфейс), соответствующий данному адресу;
2) физический адрес – MAC-адрес, например, Ethernet-адрес;
3) IP-адрес – IP-адрес, соответствующий физическому адресу;
4) тип адресного соответствия.

На рис. 2 представлен пример ARP-таблицы.

```
PS C:\Users\Alex> arp -a

Интерфейс: 192.168.0.105 --- 0x9
  адрес в Интернете      Физический адрес      Тип
  192.168.0.1           ec-43-f6-03-dd-b0     динамический
  192.168.0.121         50-46-5d-72-2e-68     динамический
  192.168.0.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.251           01-00-5e-00-00-fb     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  224.0.0.253           01-00-5e-00-00-fd     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический
  255.255.255.255       ff-ff-ff-ff-ff-ff     статический
```

Рис. 2. ARP-таблица

Разработанная программа для мониторинга сетевой активности компьютера

В среде разработки Microsoft Visual Studio 2017 Community была разработана программа определения сетевых настроек и мониторинга сетевой активности компьютера. Программа реализована на языке программирования C#.

В функциональность программы входит:

1) отображение глобальных параметров сети (название компьютера, имя пользователя, название домена, IP-адрес компьютера, IP-адрес DNS сервера, адрес MAC);

2) отображение процесса мониторинг сетевой активности (описание сетевого адаптера, скорость загрузки и передачи, количество переданных и принятых байт);

3) отображение данных таблицы ARP и таблицы маршрутизации компьютера;

4) отображение статистики работы транспортных протоколов TCP и UDP, и отображение активных TCP соединений;

5) отображение статистики протокола ICMP и эмуляция работы команды ping.

Скриншоты работы разработанной программы для мониторинга сетевой активности

1. Глобальные параметры компьютера представлены на рис. 3 и 4.

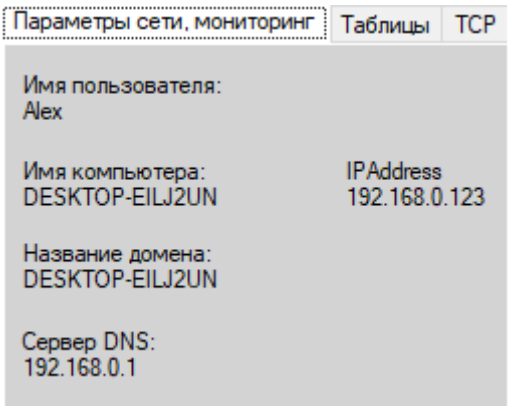

Рис. 3. Параметры компьютера

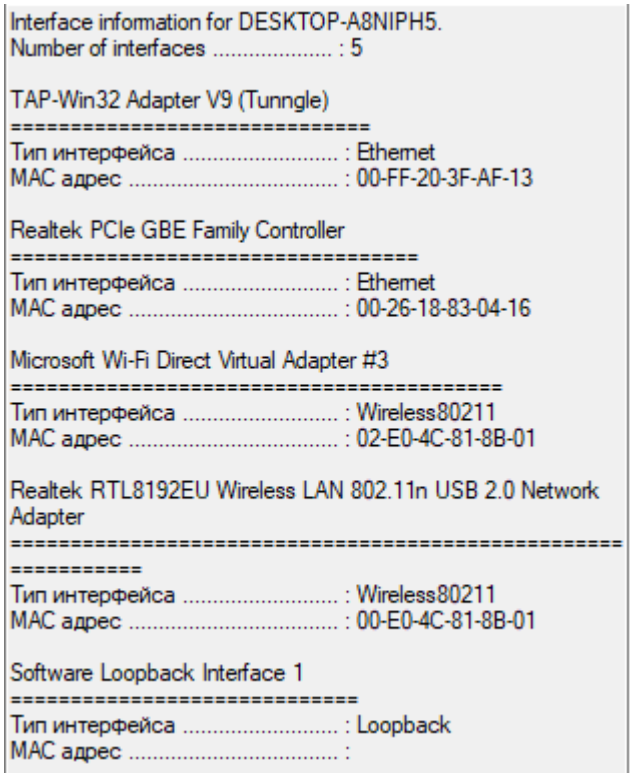

Рис. 4. Параметры компьютера: MAC адреса

2. Процесс мониторинг сетевой активности представлен на рис. 5.

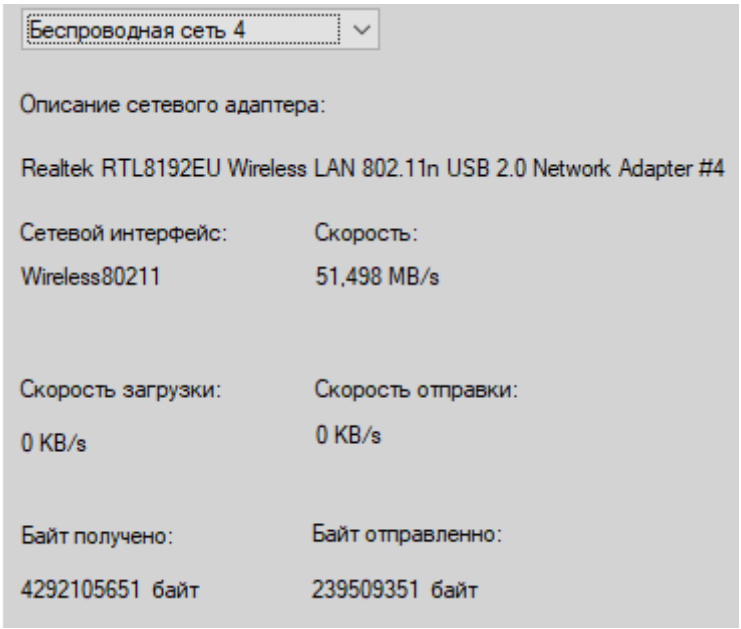

Рис. 5. Мониторинг сетевой активности

3. Данные таблицы ARP и таблицы маршрутизации компьютера представлены на рис. 6 и 7.

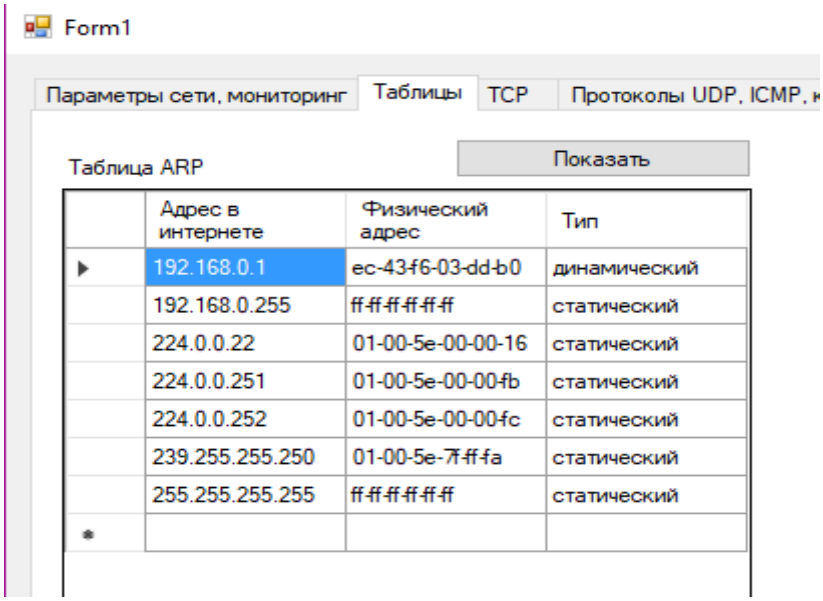

Рис. 6. Таблица ARP

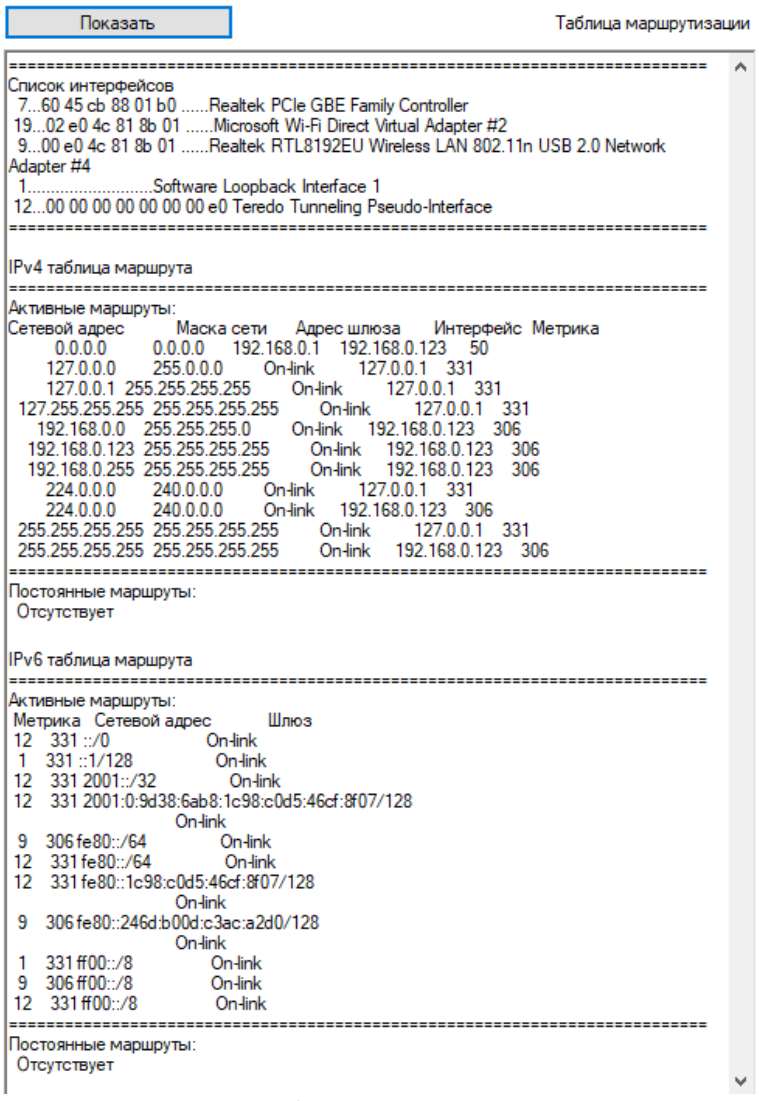

Рис. 7. Таблица маршрутизации

4. Статистика работы транспортных протоколов TCP и UDP, и активные TCP соединения представлена на рис. 8 – 11.

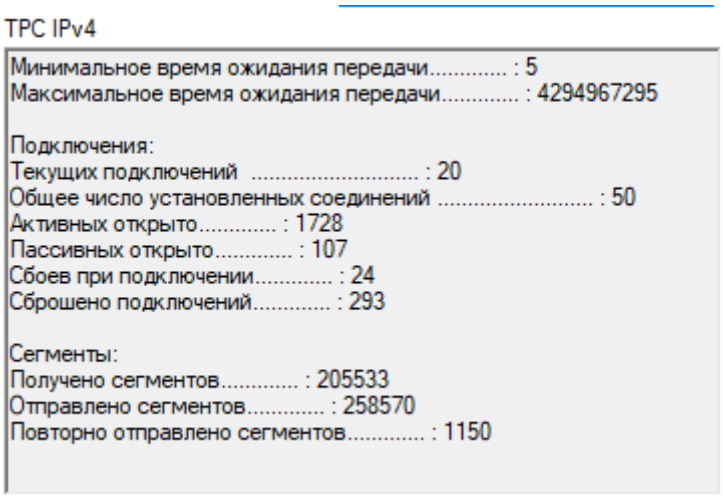

Рис. 8. Статистика работы протокола TCP IPv4

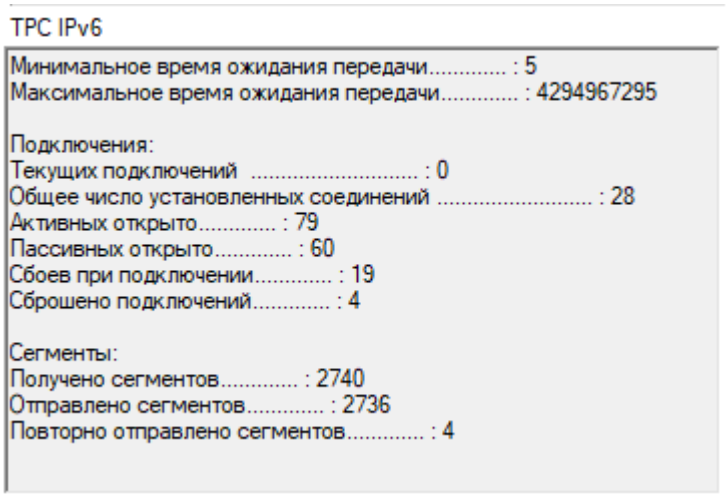

Рис. 9. Статистика работы протокола TCP IPv6

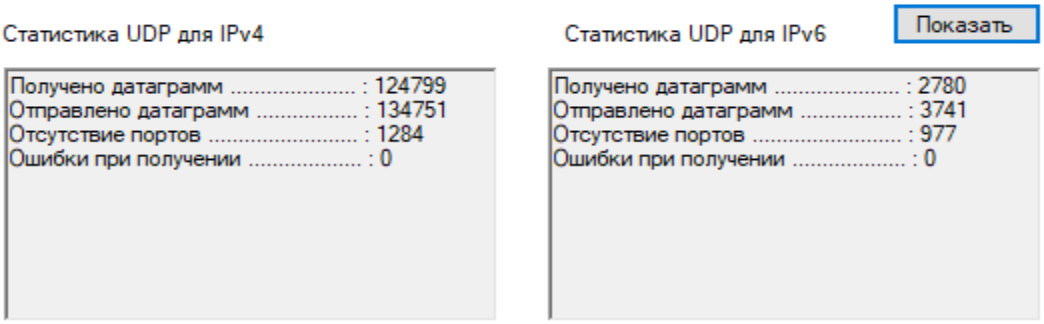

Рис. 10. Статистика работы протокола UDP

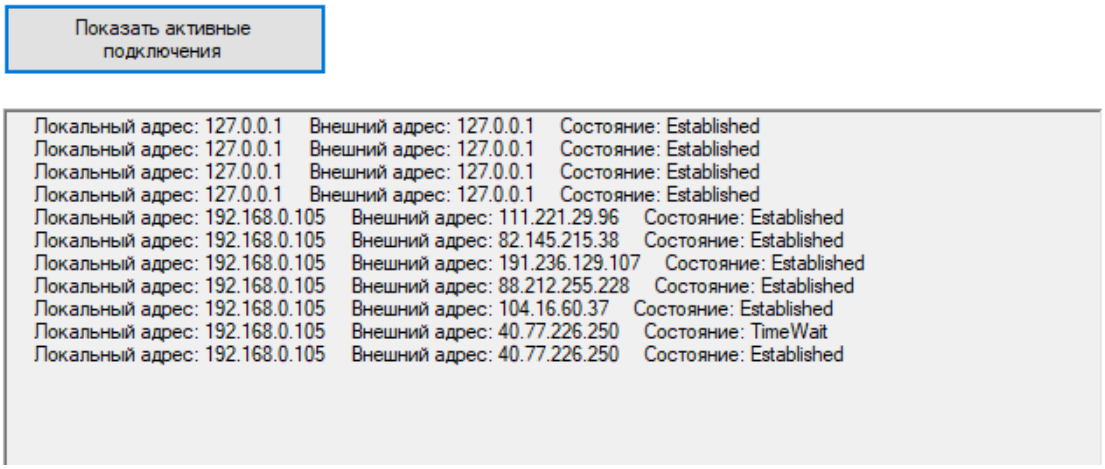

Рис. 11.Активные TCP подключения

5. Статистика протокола ICMP и эмуляция работы команды ping представлены на рисунках 12 и 13.

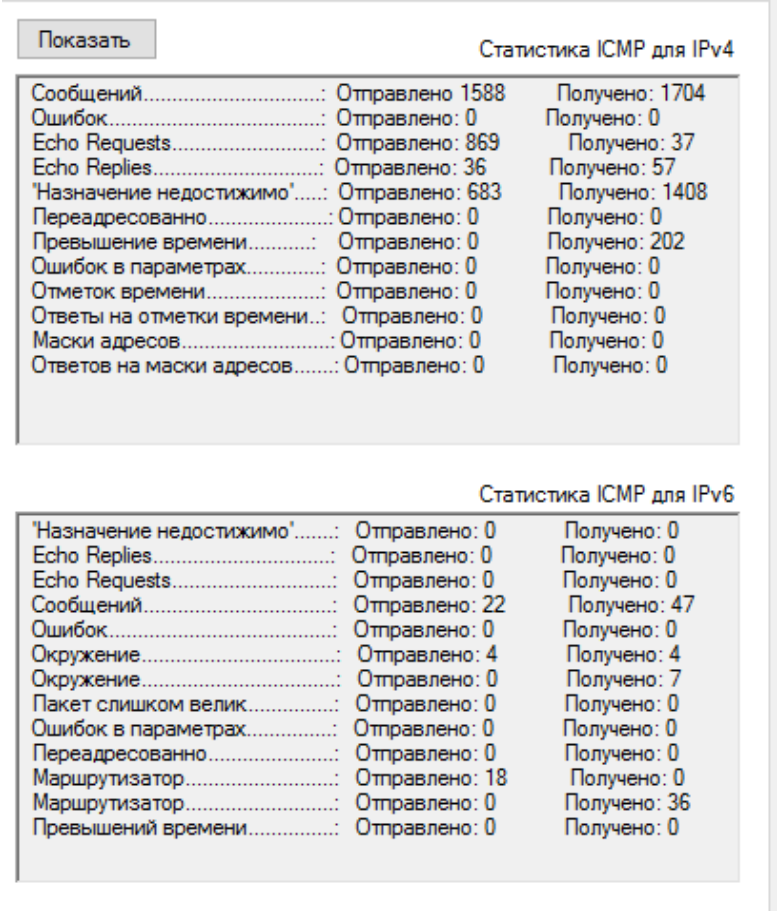

Рис. 12. Статистика работы протокола ICMP

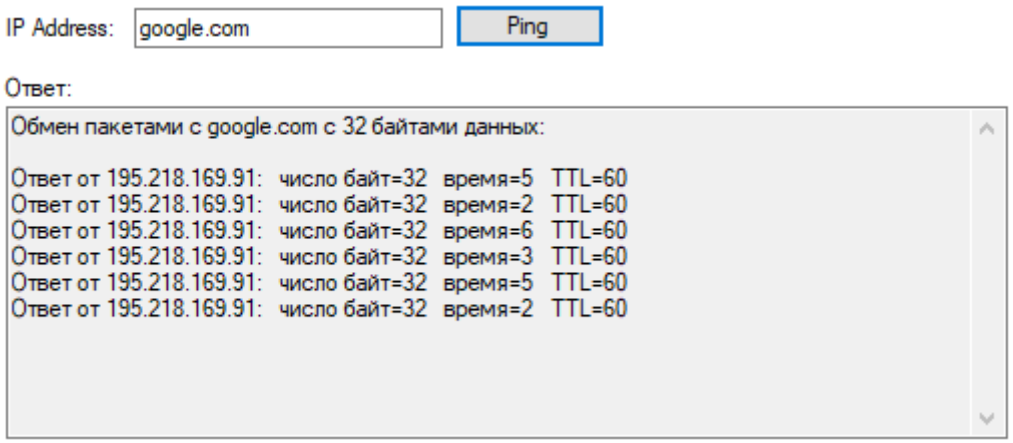

Рис. 13. Эмуляция команды ping

Список литературы

[1] Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.

[2] Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.

[3] Руководство по программированию на C# [Электронный ресурс] : «MSDN» информационный сервис для разработчиков. – Режим доступа : https://msdn.microsoft.com/ruru/library/67ef8sbd%28v=vs.120%29.aspx.