Вестник ЦЭМИ РАН. 2018-2023

ISSN 2658--3887

URL - <http://cemi.jes.su>

Все права защищены

Выпуск 2 Том 2. 2019

Частичный отказ мини-хаба при использовании в сетях

Терентьев Александр Макарович

Центральный экономико-математический институт РАН

Москва, Нахимовский проспект, 47

Аннотация

Описан случай постепенного частичного отказа мини-хаба, эксплуатирующегося в средствах сетевого мониторинга. Специфика отказа оказалась таковой, что определить её и выделить отказной элемент оказалось трудно.

Практика применения мини-хабов должна учитывать описанный случай, поскольку сфера их применения в институте достаточно широка.

Ключевые слова: локальная сеть, наблюдающая станция, мини-хаб, отказ

Дата публикации: 06.11.2019

Ссылка для цитирования:

Терентьев А. М. Частичный отказ мини-хаба при использовании в сетях // Вестник ЦЭМИ РАН. – 2019. – Т. 2. – Выпуск 2. URL: <https://cemi.jes.su/s265838870005749-6-1/>. DOI: 10.33276/S265838870005749-6

¹ Практика использования электронных устройств, в том числе в локальных сетях (хабов, роутеров, компьютеров, серверов и т.д.) порождает немало мифов об особенностях их эксплуатации. Одним из таких мифов, представляется, является мнение о том, что электронное устройство либо функционирует нормально, либо сломано и не работает вообще. В значительной степени это относится к

«простым» устройствам – сетевым коммутаторам и, конечно же, в первую очередь к хабам.

² Одно из таких простых устройств давно используется в схеме снятия результатов сетевого мониторинга [1] (рис. 1) с мониторингового порта коммутатора Cisco Catalyst-2950, являющегося распределительным центром [2] локальной сети 193.232.194.*/24 в ЦЭМИ РАН. Этим хабом являлся 10-мегабитный SURECOM EP-608\F1A (0310) 8-Port Mini Hub, вследствие чего мониторинговый порт также был установлен на скорость 10Мбит/с. Задействование этого хаба было предусмотрено с целью распределения результатов мониторинга на две наблюдающие станции (НС) в 2006 г. С течением времени, вторая НС утратила свою актуальность, в коммутаторе появилась активность гигабитных портов, а скорость мониторингового порта и указанный хаб сохранились как рудимент прежней конфигурации системы мониторинга.

Рис. 1. Схема мониторинга с 2004 г.

Начиная с середины 2014 г., основная НС начала показывать неприятную картину в виде многочисленного присутствия фрагментарных сетевых пакетов, без стандартного начала и оформленного поля кода типа пакета. На рис. 2 показана эта ситуация в формате, определённом программой показа TamView.exe [1].

Рис. 2. Примеры наблюдаемых пакетов

6 Среди четырёх пакетов только второй корректен. Пакет 3, к примеру, определён как испущенный на MAC-адрес “BC9BFFAF1C45” с MAC-адреса “5C7BD8F87F45”. Таких адресов в сети нет.

7 Разумеется, поскольку НС за MAC-адрес источника автоматически принимает байты 7-12 пакета, число «источников» очень быстро росло. Количество таких пакетов обнаруживалось пропорционально текущей скорости в локальной сети. Практически, осуществлять сетевой мониторинг стало невозможно: программная часть НС не справлялась с огромным количеством новых нод, и через несколько секунд наблюдения происходил сбой программы или MS-DOS.

8 Для объяснения причины подобного явления были рассмотрены несколько гипотез: неработоспособность компьютера с НС, неработоспособность мониторингового порта Cisco Catalyst, некорректность работы сетевого адаптера и ряд других, однако подозревать хаб в «урезании» пакетов оснований не было. Он представлялся устройством, которое если уж работает, то безотказно.

9 В процессе проверки неработоспособных устройств в конце концов упомянутый хаб был заменён на 3COM Office Connect Dual Hub-8 10/100. С этого

момента возобновился нормальный показ принимаемых пакетов. Впоследствии скорость мониторингового порта была изменена с 10Мбит на 100Мбит, причём НС продолжала работать в штатном режиме. При этом, разумеется, наблюденная скорость в сети резко возросла (рис. 3) до 8304,29 КБайт/с, т.е. порядка 8 МБайт/с, или около 64 Мбит/с. Наблюдение в это время мониторингом порта велось только от одного сервера на порту 5 Каталиста, являющегося роутером локальной сети ЦЭМИ РАН 10.0.*.* /16. Приведённые на рисунке данные выданы Мониторной программой [3], задействованной в общей цепочке выходных данных сетевого мониторинга.

¹⁰ Таким образом определено, что SURECOM EP-608\F1A (0310) 8-Port Mini Hub, не давая никакой дополнительной информации и нормально индицируя миганием лампочек коннекты, может частично выйти из строя, наводняя сеть обрывками сетевых пакетов, что приводит к перегрузке фрагментов сети и замедлению реальной скорости связи.

¹¹ При разводке сети в ЦЭМИ РАН часто используются сходные мини-хабы, вследствие чего необходима периодическая проверка истинной работоспособности фрагментов сети.

LAN Audit Monitor Station

Время МП: 03/06-19 = 17:43:33 v.1.78

Время НС: 03/06-19 = 17:40:53 v.5.23

Время SR: 03/06-19 = 17:46:55 v.2.13

IP-адрес МП: 193.232.194.13 Критерий 1с -

IP-адрес SR: 193.232.194.11 циклов до: 33000

С нач.периода НС нараст.итогом

Секунд с нач.периода 00653

Байтов всего 0147587870

Байтов пропущенных 000304488

Байтов бродкастинг 000003202

Байтов INet-From 000000000

Байтов INet-To 147099318

Байтов Inter-LAN 000488552

Активных MAC-адресов 001

001

Ср.скорость [КБ/с] 221.17

Мгн.ск. [КБ/с] 46.28 8304.29 8304.29

Цикл/с, всего 32767 32767 32767

Цикл/с,полезн 00288 08640 08640

Запол.буф.[%] 000 001 021

Посл. #отчета 0008 Max/пер Max

☒ Снимать НС при Shutdown ☐ АвтоОткл

Список исключаемых MAC-адресов

Поток исключаемых MAC-адресов

Библиография:

1. Терентьев А.М. Сетевой мониторинг. Методы и средства. Том 1: моно-графия / А.М.Терентьев. – Чебоксары: ИД «Среда», 2019. – 116 с. ISBN 978-5-6042304-9-7.
2. Терентьев А.М., Ляпичева Н.Г., Кочетова Н.А. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst. / "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 1". – Сб.статей под ред. А.М.Терентьева. – М., ЦЭМИ РАН, 2004, с.75-87, ISBN 5-8211-0317-7.
3. Терентьев А.М. Мониторная программа как средство интеграции данных наблюдающей станции в локальной сети. / "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 2". – Сб.статей под ред. М.Д.Ильменского. – М., ЦЭМИ РАН, 2005, с.6-13, ISBN 5-8211-0365-7.

Partial failures of mini-hub in local networks

Alexander Terentjev

CEMI RAS

Moscow, Nakhimovky prospect 47

Abstract

A case of gradual partial failure of a mini-hub operating in network monitoring tools is described. The specifics of the failure turned out to be such that it was difficult to determine it and isolate the abandoned element.

The practice of mini-hubs should take into account the described case, since the scope of their application at the institute is quite wide.

Keywords: local network, LAN-monitoring, mini-hub, failure

Date of publication: 06.11.2019

Citation link:

Terentjev A. Partial failures of mini-hub in local networks // Herald of CEMI. – 2019. – V. 2. – Issue 2. URL: <https://cemi.jes.su/s265838870005749-6-1/>. DOI: 10.33276/S265838870005749-6