Вестник ЦЭМИ РАН. 2013-2020

ISSN 2658--3887

URL - http://cemi.jes.su

Все права защищены

Выпуск 2 Том . 2019

Частичный отказ мини-хаба при использовании в сетях

Терентьев А. М.
Центральный экономико-математический институт РАН
Москва, Нахимовский проспект, 47

Аннотация

Описан случай постепеннного 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. Выпуск 2 [Электронный ресурс]. Доступ для зарегистрированных пользователей. URL: https://cemi.jes.su/s265838870005749-6-1/ (дата обращения: 10.02.2020). 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 мониторного 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 мониторный 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 мониторного порта и указанный хаб сохранились как рудимент прежней конфигурации системы мониторинга.

3

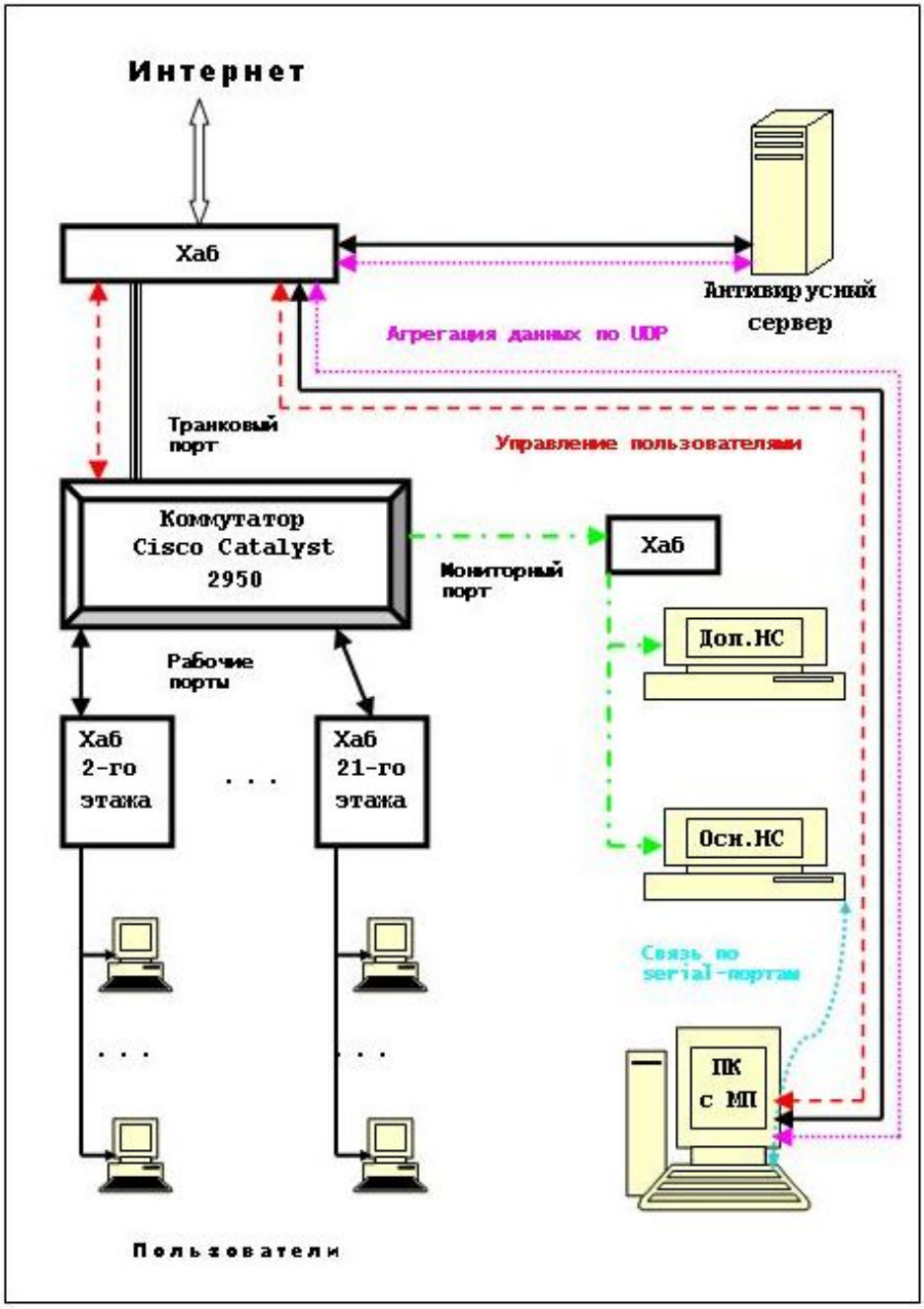

Рис. 1. Схема мониторинга с 2004 г.

4 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].

5

```
TAMVIEW.BAT - Far 2.0.1807 x86 Administrator
TAMVIEW * 1.4-2005, А.Терентьев *  Просмотр дампа пакетов  10/06-19 * 16:03:40
   Считано  пакетов:        4 Байтов:        332   MAC-Fr:Не назначен  Or:  N
   Записано пакетов:        0 Байтов:          0   MAC-To:Не назначен  Only:N
                                                   IPF:- Не назначен -  Drct:-

 !  Проверка системы и условий работы
   Проверка даты и времени... OK
   Проверка идентификации...  OK
   Проверка версии ДОС...  OK
   Прием имени программы...  OK
 : CNF=<TAMVIEW.CFG>
   Прием параметров командной строки
 : Parm=<./FI=TAMCNET.PM5 /2 /NP>
   Задан входной файл <TAMCNET.PM5>
 : 55AA 3C00   Offs= 0 (00000000h)   Pkt= 1   L= 60
   0180C2000000 000DBCBBC798 0026=802.3/?
   42 42 03 00 00 00 00 00 60 C2 00 0D BC BB C7 80   BB......`Т..╝╗╟А
   00 00 00 00 60 C2 00 0D BC BB C7 80 80 18 00 00   ....`Т..╝╗╟АА...
   14 00 02 00 0F 00 00 00 00 00 00 00 00 00 00 00   ................
 : 55AA 7700   Offs= 64 (00000040h)   Pkt= 2   L= 119
   000652324406 0015178D064F 0800=E2-IP  031.057.237.188<193.232.194.003:TCP
   45 00 00 69 3F 17 40 00 40 06 6A 96 C1 E8 C2 03   E..i?.@.@.jЦ└шТ.
   1F 39 ED BC 01 D1 8F 4B FA C5 5C 98 AC 8C 95 00   .9э╝.╤П╦┼╜Ш¬МХ.
   80 18 05 AC 41 96 00 00 01 01 08 0A A8 5F 48 8C   А..¬АЦ......и_НМ
   01 DF CF 7C 17 03 01 00 30 4D D5 A6 3D C6 E9 06   .▀╧│....0М╒ж=╞щ.
   80 E3 A6 9E 31 0B 4F 16 16 FA 61 29 43 2C 91 E0   Ауж╜1.О..·а)С,Ср
   3E 63 27 49 15 FA 4D 1A 6D 36 C0 D8 ED 42 C6 20   >с'I.·М.m6└╪эВ╞
   C4 C9 3D AE 40 0C 0B BC 80                        ─╔=о@..╝А
 : 55AA 4200   Offs= 187 (000000BBh)   Pkt= 3   L= 66
   BC9BFFAF1C45 5C7BD8FB7F45 0000=802.3/?
   C4 D6 76 7F FF 7F F3 A3 3F F8 5C E7 51 10 A5 CE   ─╓v.▄▀г?°\чQ.е╦
   D3 0F 03 3C 7F 3A 7B 6F 1D 4F 0A A6 9D AD 31 10   ╙..<▄:{о.О.ж╥н1.
   DA FF FF CC CE 00 00 FD 06 D0 AB 6F 33 43 B5 A9   г..╦╬..².╨л►о3С╡й
   AA 09 05 15                                       к...
 : 55AA 4700   Offs= 257 (00000101h)   Pkt= 4   L= 71
   CA0090DA096D 11C4BAFE2F21 0000=802.3/?
   B6 4B A8 FB F5 FF AB BD 5D FA 7B 5B A8 3B C1 A6   ╢Ки√╕.л╜]·{[и;└ж
   84 42 F5 42 DF B6 7E 43 6B 9B D6 09 82 D0 68 90   ДВ╕В▀╢~СК╝╓.В╨hР
   25 14 60 18 00 00 41 D3 04 00 30 60 00 06 EB 9D   %.`...А╙..0`..ы╥
   40 27 40 95 FA 42 C0 EA 54                        @'@х·В└ъТ

=*= <Enter> - копировать / <Space> - дальше / <Esc> - Конец
```

Рис. 2. Примеры наблюдённых 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 мониторного 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 мониторного порта была изменена с 10Мбит на 100Мбит, причём НС продолжала работать в штатном режиме. При этом, разумеется, наблюдённая 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 мониторным портом 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.

12

Рис. 3. Данные Мониторной программы

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 корпора-тивной 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 дан-ных наблюдающей станции в локальной сети. / "Развитие и использо-вание 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

A. 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. Issue 2 [Electronic resource]. Access for registered users. URL: https://cemi.jes.su/s265838870005749-6-1/ (circulation date: 10.02.2020). DOI: 10.33276/S265838870005749-6

Код пользователя: 7792; Дата выгрузки: 10.02.2020; URL - http://cemi.jes.su/s265838870005749-6-1/ Все права защищены.