

RE: Reg : Output of nProbe flow collector

Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>

Wed 11/12/2019 21:49

To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

Hi Sriram,

Regarding the fields which were not coming,

I'm giving the field name of the fields that are should be in the file in nProbe collector command. I used the template which is captured in the Wireshark to get the list of fields but what happened was like in the template the field name was just IP instead of IPV4. When I used the field name in the command like IP_SRC_ADDR the nProbe was not able to identify the field and ignored the corresponding value. So I just had field which doesn't have IPV4 in it's name.

And another was for BYTES and PKTS .In the Wireshark captured template it was just BYTES and PKTS but the field name which nProbe knows – IN_BYTES and IN_PKTS.

I assumed that the nProbe would correlate the field name with the field names sent in the template

Fields sent in the template :

```
> Frame 132: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: ca:02:00:7d:00:00 (ca:02:00:7d:00:00), Dst: PcsCompu_dd:91:f4 (08:00:27:dd:91:f4)
> Internet Protocol Version 4, Src: 192.168.56.105, Dst: 192.168.56.106
> User Datagram Protocol, Src Port: 62087, Dst Port: 2055
Cisco NetFlow/IPPFIX
  Version: 9
  Count: 1
  SysUpTime: 1496.420000000 seconds
  Timestamp: Dec 10, 2019 22:44:41.000000000 India Standard Time
  FlowSequence: 56
  SourceId: 0
  FlowSet 1 [Id=0] (Data Template): 256
    FlowSet Id: Data Template (V9) (0)
    FlowSet Length: 40
    Template (Id = 256, Count = 8)
      Template Id: 256
      Field Count: 8
      > Field (1/8): IP_SRC_ADDR
      > Field (2/8): IP_DST_ADDR
      > Field (3/8): L4_SRC_PORT
      > Field (4/8): L4_DST_PORT
      > Field (5/8): IP_TOS
      > Field (6/8): PROTOCOL
      > Field (7/8): BYTES
      > Field (8/8): PKTS
```

Only the fields L4_SRC_ADDR, L4_DST_ADDR and PROTOCOL was getting inserted in the file.

Field name supposed to be given	Field name given by me
IPV4_SRC_ADDR	IP_SRC_ADDR
IPV4_DST_ADDR	IP_DST_ADDR
L4_SRC_PORT	L4_SRC_PORT
L4_DST_PORT	L4_DST_PORT
PROTOCOL	PROTOCOL
IPV4_TOS	IP_TOS
IN_BYTES	BYTES
IN_PKTS	PKTS

Then I changed the field name accordingly and I'm able to get the value for all the fields.

Kindly ignore the message sent in Teams.

Thanks and Regards,
Lavanya Singaravelan

From: Lavanya Singaravelan**Sent:** 11 December 2019 14:34**To:** Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>**Subject:** Reg : Output of nProbe flow collector

Hi Sriram,

Please find the output I'm getting for the nProbe flow collector from the below attached screenshots.

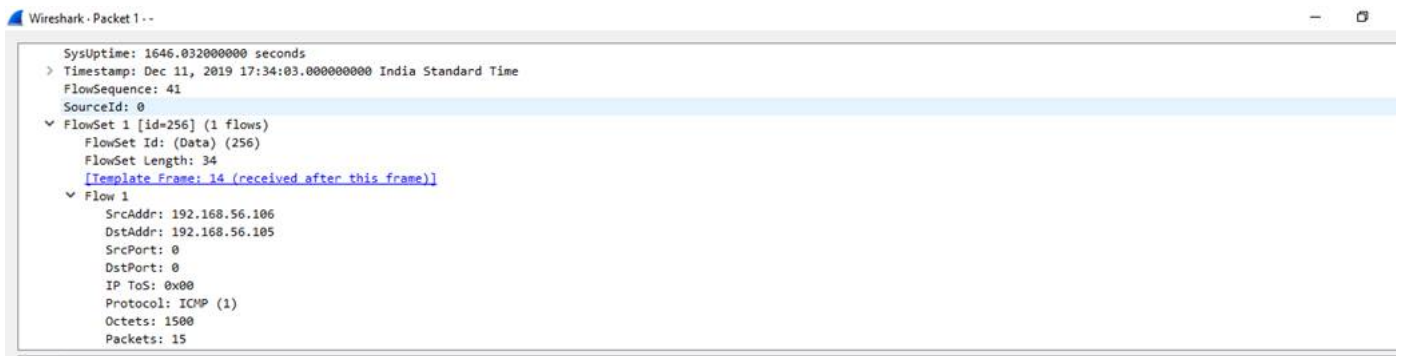
From Cisco 7200 router:

```
Router1#sh ip cache flow
IP packet size distribution (15 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

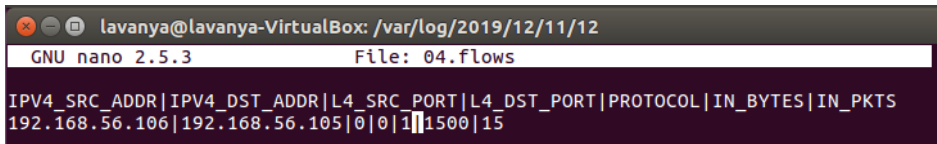
 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
 1 active, 65535 inactive, 1 added
 5 ager polls, 0 flow alloc failures
 Active flows timeout in 1 minutes
 Inactive flows timeout in 20 seconds
IP Sub Flow Cache, 533256 bytes
 0 active, 16384 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 0 chunks added
 last clearing of statistics 00:00:10
Protocol      Total    Flows  Packets Bytes  Packets Active(Sec) Idle(Sec)
-----
              Flows   /Sec   /Flow /Pkt   /Sec   /Flow   /Flow
SrcIf      SrcIPaddress  DstIf      DstIPaddress  Pr SrcP DstP  Pkts
Fa0/0      192.168.56.106 Local      192.168.56.105  01 0000 0000   15
```

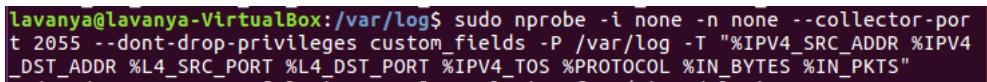
In the WireShark :



In the nProbe collector file:



The command used for nProbe collector side :



Thanks and Regards,
Lavanya Singaravelan