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>

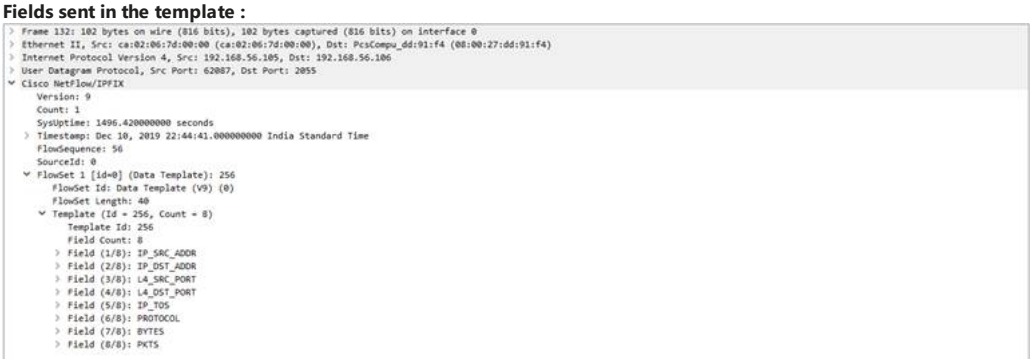
Hi Sriram,

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 :



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.

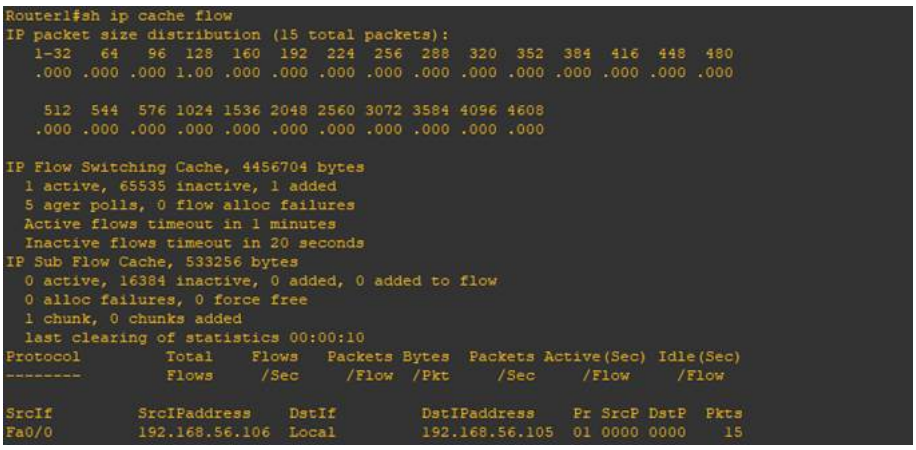
Thanks and Regards,
Lavanya Singaravelan

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

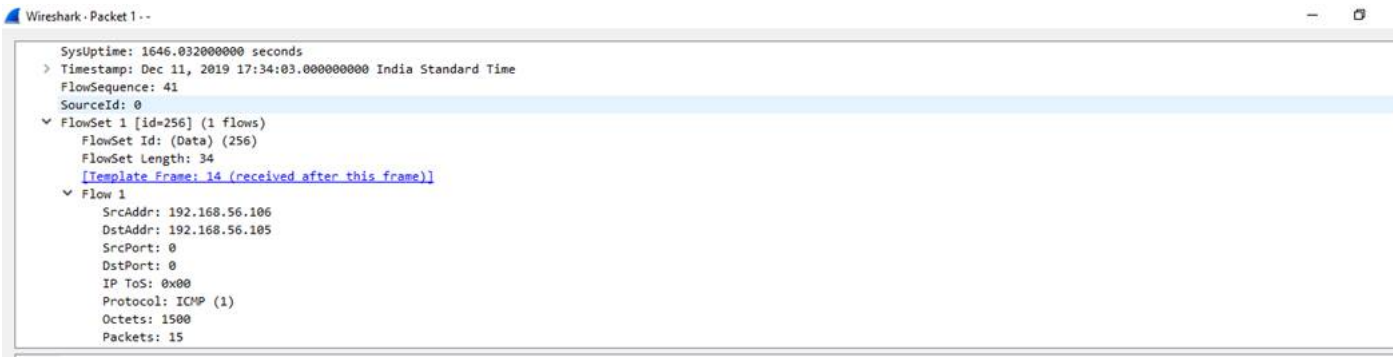
Hi Sriram,

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

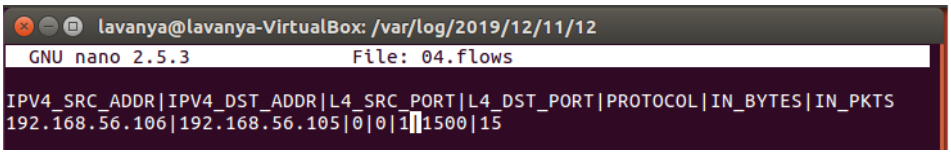
From Cisco 7200 router:



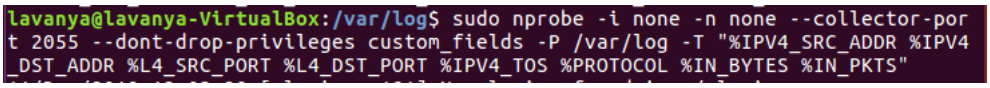
In the WireShark :



In the nProbe collector file:



The command used for nProbe collector side :



Thanks and Regards,
Lavanya Singaravelan