ILLINOIS INSTITUTE OF TECHNOLOGY

Integration and Tutorial of pmacct Toolset into FABRIC Testbed

Pilar Fernandez Gayol, Nik Sultana

Introduction and Motivation

- The **FABRIC** testbed empowers experimentation and research on a large scale, facilitating cutting-edge exploration and innovation in networking.
- **pmacct** is a set of widely-used, multi-purpose passive monitoring tools for data networks.
- pmacct's ability to perform multifunctional network monitoring can benefit users of the FABRIC testbed infrastructure, enabling detailed, real-time monitoring of network traffic in an **advanced research environment.**
- Creating a tutorial on pmacct integration in the FABRIC testbed also cultivates interdisciplinary **learning** among **students**, facilitating knowledge exchange in network monitoring.

Future Work

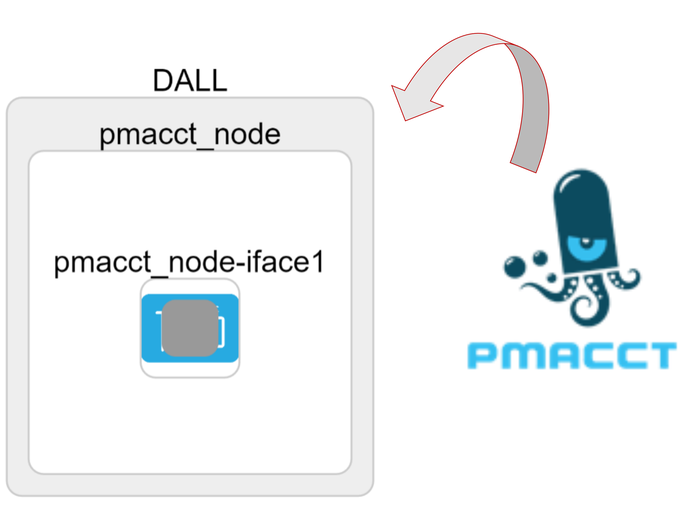
- Results will be presented in both a web tutorial, providing step-by-step instructions on utilizing pmacct in a FABRIC testbed environment, and a detailed report documenting the entire process followed, from initial research to implementation and findings.

Acknowledgement

Dale Carder (ESnet) and Paolo Lucente (pmacctd)

Approach

- We carried out an in-depth study of the pmacct toolset, examining its features, functionalities, and architecture.
- Deployed a FABRIC experiment to verify pmacct's capability in analyzing both live network traffic and .pcap files.
- Thorough testing will ensure pmacct's effectiveness in multiple scenarios within the FABRIC testbed. Upon completion, the project will provide insights into pmacct's performance in this environment.
- Realization of an educational tutorial, aimed at providing users with practical guidance on utilizing pmacct within the FABRIC testbed environment.




```
SRC_IP,DST_IP,SRC_PORT,DST_PORT,PROTOCOL,PACKETS,BYTES
192.168.1.101,178.123.13.120,42559,26895,udp,1,95
208.117.231.17,192.168.1.101,443,56561,tcp,71,102240
192.168.1.101,208.117.231.17,56562,443,tcp,47,2212
208.117.231.17,192.168.1.101,443,56562,tcp,54,77760
192.168.1.101.208.117.231.17.56561.443.tcp.53.2444
208.117.231.17,192.168.1.101,443,56563,tcp,63,90720
178.123.13.120,192.168.1.101,26895,42559,udp,1,98
192.168.1.101,208.117.231.17,56563,443,tcp,45,2188
93.184.221.133,192.168.1.101,80,56668,tcp,15,20212
192.168.1.100,239.255.255.250,54714,1900,udp,2,322
192.168.1.101,90.84.59.130,56671,443,tcp,4,161
192.168.1.101,93.184.221.133,56668,80,tcp,11,501
192.168.1.101,173.194.35.53,56643,443,tcp,21,5083
```

(Evidence of pmacct integration success)

```
daemonize: false
debug: true
pcap_savefile: gmail.pcapng.cap

aggregate: src_host, dst_host, src_port, dst_port, prot

plugin_buffer_size: 4096
plugins: print

print_output: csv
print_output_file: result.txt
print_history_roundoff: m
```

```
ubuntu@pmacctnode:~/pmacct-1.7.8$ sudo pmacctd -f pmacct.conf
INFO ( default/core ): Promiscuous Mode Accounting Daemon, pmacctd 1.7.8-git (RELEASE)
INFO ( default/core ):  '--enable-l2' '--enable-traffic-bins' '--enable-bgp-bins' '--enable-bmp-bins'
INFO ( default/core ): Reading configuration file '/home/ubuntu/pmacct-1.7.8/pmacct.conf'.
INFO ( default/core ): [,0] link type is: 1
INFO ( default_print/print ): plugin_pipe_size=4096000 bytes plugin_buffer_size=4096 bytes
INFO ( default_print/print ): ctrl channel: obtained=212992 bytes target=8000 bytes
INFO ( default/core ): PCAP capture file, sleeping for 2 seconds
INFO ( default_print/print ): cache entries=16411 base cache memory=54878384 bytes
INFO ( default_print/print ): *** Purging cache - START (PID: 64898) ***
INFO ( default_print/print ): *** Purging cache - END (PID: 64898, QN: 106/106, ET: 0) ***
INFO ( default/core ): OK, Exiting ...
```

(Execution example)