---

17 May 2019

GUIDE: Enable Packet Capture

Each interface on the 128T router can perform packet capture functions, to record traffic to persistent storage for troubleshooting purposes. Within the device-interface configuration, administrators may set a capture filter, using [128T Berkeley Packet Filter Syntax Guide](https://community.128technology.com/viewdocument/128t-berkeley-packet-filter-syntax-guide?CommunityKey=4c0e5fb2-7f15-41a4-9b0a-fa1b8b61f863&tab=librarydocuments), to specify which packets to capture and record. (The 128T router uses a subset of the overall BPF grammar; for a comprehensive list of the supported BPF grammar, please refer to the [128T Configuration Reference Guide 3.2](https://community.128technology.com/viewdocument/128t-configuration-reference-guide-3-2?CommunityKey=4c0e5fb2-7f15-41a4-9b0a-fa1b8b61f863&tab=librarydocuments).)

In order to turn on packet capture on a device-interface, just add your filter to the capture-filter field.

We’ll start with a simple example, capture all packets on device-interface 10:

admin@conductor1.nycsite1# configure authority router seattlesite1

admin@conductor1.nycsite1 (router[name=seattlesite1])# node branchoffice1

admin@conductor1.nycsite1 (node[name=branchoffice1])# device-interface 10

admin@conductor1.nycsite1 (device-interface[name=10])# capture-filter len>0

admin@conductor1.nycsite1 (device-interface[name=10])# show

name 10

type ethernet

pci-address 0000:00:04.0

**capture-filter len>0**

network-interface dc1

 name dc1

 global-id 1

 type external

 inter-router-security aes1

 address 10.0.128.0

 ip-address 10.0.128.0

 prefix-length 31

 gateway 10.0.128.1

 exit

 adjacency 10.0.128.1

 ip-address 10.0.128.1

 peer bostonsite1

 inter-router-security aes1

 exit

exit

Capturing will begin once this configuration is committed.

The capture files are stored in the standard PCAP format, and are placed in the same default location as the 128T router’s log files: **/var/log/128technology**

[t128@conductor ~]$ ls -al /var/log/128technology/128T\*

-rw-r--r--     1 root root 131153 Mar 29 19:38 /var/log/128technology/128T\_10.pcap

-rw-rwxr--+ 1 root root         24 Mar 26 18:44 /var/log/128technology/128T.pcap

An interface may have multiple capture-filter arguments specified. When more than one are configured, a packet will be captured into the PCAP file if **ANY** of the criteria are matched (logically, capture-filter elements are joined with an “or”; i.e., statement1 or statement2 or statement3, etc.).

To disable the packet capture feature, just remove the capture-filter:

admin@conductor1.nycsite1# configure authority router seattlesite1

admin@conductor1.nycsite1 (router[name=seattlesite1])# node branchoffice1

admin@conductor1.nycsite1 (node[name=branchoffice1])# device-interface 10

admin@conductor1.nycsite1 (device-interface[name=10])# delete capture-filter len>0

Are you sure you want to delete values ['len>0'] from list 'capture-filter'? [y/N]: y