|  |  |  |  |
| --- | --- | --- | --- |
| Basic Syntax | | | |
| pktmon filter list | List all packet filters | **pktmon status** | Query Packet Monitor status |
| pktmon filter add | Add a packet file | **pktmon counters** | List all counters |
| pktmon filter remove | Remove a packet filter | **pktmon reset** | Reset all counters to zero |
| pktmon start | Start capturing to file | **pktmon etl2pcap** | Covert ETL file format to pcapng |
| pktmon stop | Stop capturing to file | **pktmon unload** | Unload pktmon driver |

|  |  |
| --- | --- |
| Filter Syntax | |
| pktmon filter add [<name>] [-m mac [mac2]] [-v vlan] [-d { IPv4 | IPv6 | number }] [-t { TCP [flags...] | UDP | ICMP | ICMPv6 | number }]  [-i ip [ip2]] [-p port [port2]] [-e [encapsulation]] | |
| Packets must match ALL conditions *from at least ONE filter* to be logged | |
| pktmon filter add -p 53 | Add port 53 (TCP and UDP, IPv4 and IPv6) to filter list |
| pktmon filter add -t TCP -p 22 | Add only TCP port 22 to filter list |
| pktmon filter add -p 123, 123 | Only packets with src port 123 and dst port 123 |
| pktmon filter add -i 172.32.1.1 | Only packets to/from IP 172.31.1.1 |
| pktmon filter add -i 172.32.1.1, 8.8.8.8 | Only packets between these two IPs |
| pktmon filter add -m ba:ad:be:ef:00:01 | Only packets with MAC BA:AD:BE:EF:00:01 |
| pktmon filter add -v 200 | Only packets with VLAN 200 in 802.1Q header |
| pktmon filter add -e <VXLAN|GRE|NVGRE…> | Only packets with specific encapsulation |
| pktmon filter list | List all filters |
| pktmon filter remove | Remove **all** filters |

|  |  |
| --- | --- |
| Capture Syntax | |
| pktmon start [-c [--comp { all | nics | [ids...] } ] [--pkt-size { 0 | size} ]  [--type { all | flow | drop } ]] [-f file-name] [-s file-size]  [-r] [-m { circular | multi-file | memory | real-time } ] | |
| pktmon start -c | Log ALL network interfaces to PktMon.etl |
| pktmon comp list | Get a list of network interface IDs |
| pktmon start -c --comp 13 | Capture from only network interface ID 13 |
| pktmon start -c –-pkt-size 0 | Capture FULL packet data (default 128 bytes, 0 == FULL) |
| pktmon start -c --type drop | Only log dropped packets |
| pktmon start -c -f output.etl | Specify non-default filename for ETL log |
| pktmon start -c -s 1024 | Set max size (MB) of output file (512 MB default) |
| pktmon start -c -r | When the ETL file is full, overwrite beginning |
| pktmon start -c -m multi-file | When the ETL file is full, create a new file (default is circular) |
| pktmon stop | Stop capture packets: output in pktmon.etl |

|  |  |
| --- | --- |
| Output Syntax | |
| pktmon etl2txt <etl file> -o <txt file> | Convert ETL file to TXT |
| pktmon etl2pcap <etl file> -o <pcap file> | Convert ETL file to PCAPNG (wireshark) format |
| pktmon etl2pcap <etl file> -o <pcap file> -d | “-d” == Only convert DROPPED packets |