|  |  |  |  |
| --- | --- | --- | --- |
| Basic Syntax | | | |
| pktmon filter list | List all packet filters | **pktmon comp list** | List active components |
| pktmon filter add | Add a packet filter | **pktmon comp counters** | List all counters |
| pktmon filter remove | Remove a packet filter | **pktmon reset** | Reset all counters |
| pktmon start | Start capturing to file | **pktmon format** | Covert ETL file format |
| pktmon stop | Stop capturing to file | **pktmon unload** | Stop pktmon service |

|  |  |
| --- | --- |
| 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 [port]] | |
| Packets much 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 component ID]  [-d] [--etw [-p size] [-k keywords]]  [-f] [-s] [-r] [-m] | | Acquire component ID from *pktmon comp list* |
| pktmon start --etw | Log ALL network interfaces to PktMon.etl | | |
| pktmon start --etw -c 13 | Capture from only component ID 13 | | |
| pktmon start --etw -p 0 | Capture FULL packet data (default 128 bytes) | | |
| pktmon start --etw -d | Only log dropped packets | | |
| pktmon start --etw -f output.etl | Specify non-default filename for ETL log (default PktMon.etl) | | |
| pktmon start --etw -s 1024 | Set max size (MB) of output file (512 MB default) | | |
| pktmon start --etw -r | When the ETL file is full, overwrite beginning | | |
| pktmon start --etw -m | When the ETL file is full, create a new file | | |
| pktmon stop | Stop capture packets | | |

|  |  |
| --- | --- |
| Output Syntax | |
| pktmon format <etl file> -o <txt file> | Convert ETL file to TXT |
| pktmon pcapng <etl file> -o <pcap file> | Convert ETL file to PCAPNG (wireshark) format |
| pktmon pcapng <etl file> -o <pcap file> -d | “-d” == Only convert DROPPED packets |
| pktmon pcapng <etl file> -o <pcap file> -c 13 | Only convert packets from component ID 13 |