**PCAP CHEAT SHEET**

**USAGE NOTES:**

* Berkeley capture filters referenced here, as these are applicable to VIRL packet captures
* Wireshark display filters tested on Mac version 2.4.2

|  |  |  |
| --- | --- | --- |
| **Traffic type** | **Capture filter(s) [Berkeley]** | **Display filter(s) [wireshark]** |
| RIPv2 | udp port 520 | udp.port==520 |
| EIGRP | ip proto eigrp | ip.proto==88 |
| OSPF | ip proto ospf | ip.proto==89 |
| LDP | udp port 646 or tcp port 646 | udp.port==646 or tcp.port==646 |
| PIM | ip proto pim | pim |
| IGMP | ip proto igmp | igmp |
| BGP | tcp port 179 | tcp.port==179 |
| ICMP | ip proto icmp | icmp |

**Wireshark display filter operands**

|  |  |
| --- | --- |
| and | && |
| or | or |
| = | == |
| protocol and port | ip.port== udp.port== tcp.port== |
| source or dest ip | ip.src== ip.dst== |

**Useful links:**

Berkeley packet filters: <http://biot.com/capstats/bpf.html>

Wireshark display filters: <https://wiki.wireshark.org/DisplayFilters>