Using the Monitor Traffic Matching Command Syntax

Turbo Boost Your Packet Capture

The monitor commands in the Junos® OS are powerful ways to capture and examine packets of interest. The monitor traffic matching command examines traffic destined for the Routing Engine that matches certain parameters based on regular expressions. You can use the monitor traffic command to specify an expression using the matching option and including the expression in quotation marks: `user@host> monitor traffic matching "expression"`

You can use all sorts of matching conditions but you can also use relational operators to compare arithmetic expressions. For example: `monitor traffic matching "ether[0] & 1 != 0"` captures all multicast traffic, but the syntax may not be immediately obvious. In this case, the packet's first Ethernet byte is examined (`ether[0]`), then logically *ANDed* with a value 1 (`& 1`). So, if the result is *NOT EQUAL* to 0 (`!= 0`), then the logical operation is *TRUE* (`= 1`), and so then this is a multicast frame to be captured. (Multicast frames must have the "first bit on the wire" set to 1.)

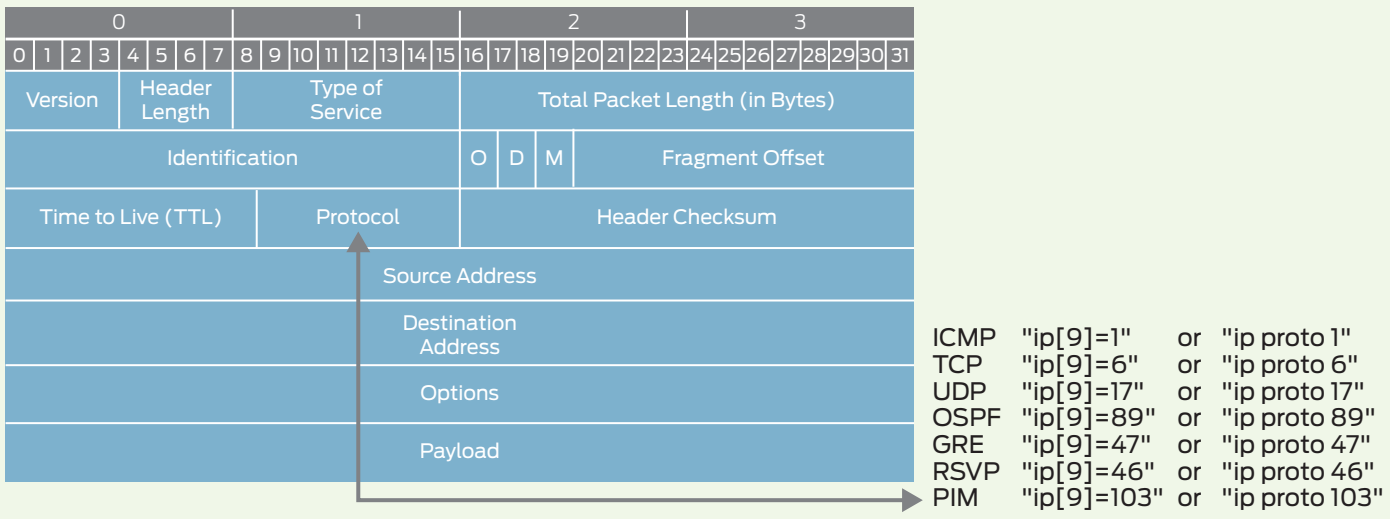
Examples:

- To match on the LAN L1 ISIS hello traffic:
  `monitor traffic matching "((ether[21]=15) and iso)"`
- To match on the LLDP traffic:
  `monitor traffic matching "(ether[12:2]=0x88cc)"`
- Either of the following expressions match on the PIM protocol:
  `monitor traffic matching "ip[9]=103" or monitor traffic matching "ip proto 103".`
  The "or" notation is represented in the poster's table as the "|" symbol. To capture RARP traffic in the table as "ether proto \rarp | ether proto 0x8035 | ether[12:2]=0x8035" the expression can be:
  `monitor traffic interface g-0/0/1 matching "ether proto \rarp"`
  or `monitor traffic interface g-0/0/1 matching "ether proto 0x8035"`
  or `monitor traffic interface g-0/0/1 matching "ether[12:2]=0x8035".`
  All expressions have the same effect on the command.

Notes

- Don't confuse this command with the `monitor interface traffic` command, which is similar but used to display real-time interface statistics in one second intervals.
- Captures can degrade device performance.
- Only device traffic can be analyzed, not transit traffic.
- Monitor traffic command is not supported on QFabric®.
- DNS delays can be eliminated with the no-resolve option.

An Example Matching for the IPv4 Packet Header



Matching Expressions Across the Application, Transport, Network, and Network Access Layers

This is TCP/IP layering, not OSI-RM layering. This table shows basic and IS-IS values.

Application Layer	**TCP and UDP** DNS tcp udp (port 53) LDP tcp udp (port 646) SNMP server: tcp udp (port 161) traps: tcp udp (port 162) **TCP Only** BGP (tcp port 179) FTP date (tcp port 20) control (udp port 21) TELNET (tcp port 23) DHCP server (udp port 67) client (udp port 68) (IPv4 only)	**UDP Only** BFD single hop (udp port 3784) multi-hop (udp port 4784) micro (udp port 6784) NTP (udp port 123) RIP (udp port 520) DHCPv6 server (udp port 547) client (udp port 546) (IPv6 only)	
Transport Layer	**TCP Only** TCP ([ip | ip6] proto 6 | tcp | ip[9]=6 | ip6[6]=6)	**UDP Only** UDP ([ip | ip6] proto 17 | udp | ip[9]=17 | ip6[6]=17)	
Network Layer	EIGRP ([ip] proto 88 | ip[9]=88) OSPF ([ip] proto 89 | ip[9]=89) VRRP ([ip] proto 112 | ip[9]=112) GRE ([ip] proto 47 | ip[9]=47) RSVP ([ip] proto 46 | ip[9]=46) PIM ([ip] proto 103 | ip[9]=103) **IPv4** IPv4 (ether proto \ip | ether proto 0x0800 | ether[12:2]=0x0800 | ip) ICMP ([ip] proto 1 | icmp | ip[9]=1) ICMP echo (icmp[icmptype]=8 | icmp[0]=8) ICMP reply (icmp[icmpcode]=0 | icmp[1]=0) ICMP unreachable&DF set (icmp[0]=3 and icmp[1]=4)	OSPFv3 (ip6 proto 89 | ip6[6]=89) VRRPv3 (ip6 proto 112 | ip6[6]=112) **IPv6** IPv6 (ether proto \ip6 | ether proto 0x86dd |ether[12:2]=0x86dd | ip6) ICMPv6 ([ip6] proto 1 | icmp6 | ip6[6]=58) ICMPv6 echo (ip6[40:2]=0x8000) ICMPv6 reply (ip6[40:2]=0x8100) IPv6 Router Advertisement (ip6[40:2]=0x8600)	**IS-IS Packet Examples** LAN L1 Hello ((ether[21]=15) and iso) LAN L2 Hello ((ether[21]=16) and iso) P2P Hello ((ether[21]=17) and iso) L1 LSP ((ether[21]=18) and iso) L2 LSP ((ether[21]=20) and iso) L1 CSNP ((ether[21]=24) and iso) L2 CSNP ((ether[21]=25) and iso) L1 PSNP ((ether[21]=26) and iso) L2 PSNP ((ether[21]=17) and iso)
Network Access Layer	802.1Q (ether[12:2]=0x8100) LLDP (ether[12:2]=0x88cc) RARP (ether proto \rarp | ether proto 0x8035 | ether[12:2]=0x8035) ARP (ether proto \arp | ether proto 0x0806 | ether[12:2]=0x0806) MPLS (ether proto 0x8847 | ether[12:2]=0x8847 | mpls) ICMP encapsulated in MPLS (mpls and icmp)		CDP (ether dst 01:00:0c:cc:cc:cc) STP (ether dst 01:80:c2:00:00:00) ISIS (iso)
	Ethernet-II (ethertype ether[12:2]>=0x0600 or 1536)		802.3 (length:ether[12:2]<=0x05DC or 1500)

- The Layer 2 header can be seen on inbound link layer protocol traffic, but the IP and MPLS traffic Layer 2 header will be stripped off.
- Use a size of at least 1531 to monitor IS-IS packets and capture the full packet.
- The hidden parameter write-file can save the captured traffic into a file for analyis in Wireshark. For example, monitor traffic interface ge-1/0/1 matching mpls write-file /var/tmp/mpls-capture.pcap.
- [ip] proto 6 | tcp means you can use "matching tcp" or matching "ip proto 6" or matching "proto 6"
- proto 6 = (ip proto 6) or (ip6 proto 6).
- port 53 = (tcp port 53) or (udp port 53).
- ether[12,2] means start at offset 12 into the Ethernet header and read 2 bytes.
- ip[9] is the same as ip[9:1] which describes the protocol.
- Here, in ether proto \arp[ip | rarp], the backslash (\) is used only to match inside the Ethernet header since IP, ARP, and RARP can also be used in independent match conditions.
- Except for 802.1Q and LLDP, if there is VLAN traffic then ether[12:2] will be ether[16:2]. For example, ARP traffic inside a VLAN can be captured by ether[16:2]=0x0806, so when using ether proto \arp there's no need to calculate the Ethernet header offset.

This poster complements the complete documentation for the monitor traffic matching command at the Juniper TechLibrary: https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/command-summary/monitor-traffic.html

Poster concept: Rick Zhang, Walter Goralski.

DAY ONE POSTER

Juniper Networks Information and Learning Experience (iLX)

www.juniper.net/posters