IOS Packet Capture Reference Sheet

BlameTheNetwork.com

IOS Platforms:

IOS 12.4(20)T or later & IOS-XE 15.2(4)S - 3.7.0 or later

The Following is for IOS - IOS-XE Follows a few differences.

1. Create the Buffer

monitor capture buffer BUF circular

2. Create an access list to specify what traffic to capture

ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1

3. Attach the access list to your capture buffer

monitor capture buffer BUF filter access-list BUF-FILTER

4. Create a Point and assign to the interface to capture on

monitor capture point ip cef POINT fastEthernet 0 both

5. Associate the capture buffer and capture point

monitor capture point associate POINT BUF

---

6. Start the capture point | Stop capture when finished

monitor capture point start POINT
monitor capture point stop POINT

 # View metrics and dump if desired before exporting

show monitor capture buffer BUF parameters
show monitor capture buffer BUF dump

7. Export the capture to analyze with wireshark or equiv.

monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap

Full Usage Syntax

monitor capture [buffer size size] [circular | linear] [dot1q] [filter acl-num | exp-acl-num | aclname] [length bytes] {clear [filter] | export buffer location | schedule at hh : mm : ss [date [month year]] | start [for number {seconds | packets}]} | stop}