Capturing L2 traffic in LibPcap format ("tcpdump") on Cisco IOS

Hardware: 7200, Dynamips
Software: IOS Version 15.2(4)S3

Extra notes: http://www.routereflector.com/2013/05/embedded-packet-capture-tcpdump-on-cisco-ios-routers/

This functionality is also supported on ASA, ASR and NX-OS. The funtionality and syntax will vary slightly however.

1. Create an ACL to classify the Ingress traffic

```
R2(config)#ip access-list standard dump
R2(config-std-nacl)#permit 10.0.0.0 0.0.0.255
```

2. Bind a memory buffer to the ACL for storing the captured data

```
R2# monitor capture buffer BUFFER size 512 max-size 256 circular
R2# monitor capture buffer BUFFER filter access-list dump
```

3. Define which interfaces must be monitored and where store data

```
R2# monitor capture point ip cef CAPTURE FastEthernet1/0 both
R2# monitor capture point associate CAPTURE BUFFER
```

→ so here the Pcap compliant records will be exported to in the filename "CAPTURE.pcap".

4. The capture must be started and stopped when not needed anymore

```
start:
R2# monitor capture point start CAPTURE

and once the data has been gathered, stop:
R2# monitor capture point stop CAPTURE
```

5. Transer the capture file for analysis

```
R2# monitor capture buffer BUFFER export tftp://10.0.0.2/CAPTURE.pcap
```

Note: do not forget to create the file first if required by the tftp – server.

Examine locally in eg Wireshark or tcpdump:

```
$ tcpdump -vvvX -r CAPTURE.pcap
22:47:58.035915 IP (tos 0x0, ttl 63, id 17015, offset 0, flags [none], proto
ICMP (1), length 84)
    10.0.0.2 > 10.0.0.1: ICMP echo request, id 12810, seq 0, length 64
     0x0000:  4500 0054 4277 0000 3f01 2530 0a00 0002  E..TBw..?.%0....
     0x0010:  0a00 0001 0800 7333 320a 0000 5595 875e  ......s32...U..^
     0x0020:  0000 8acb 0809 0a0b 0c0d 0e0f 1011 1213  ................
     0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
     0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
     0x0050:  3435 3637                                4567
```

6. Or examine the contents locally (limited functionality)

```
R2# show monitor capture buffer BUFFER dump
```

For the CSR1000V, the commands are sligthly different:

```
csr10000v(config)#ip access-list extended Monitored-Host
```

```
csr10000v(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 any

csr10000v#monitor capture mycap access-list Monitored-Host
csr10000v#monitor capture mycap limit duration 1000     note: [seconds]
csr10000v#monitor capture mycap interface gi1 both      note: [in/out]
csr10000v#monitor capture mycap buffer circular size 10 note: [MB]
csr10000v#monitor capture mycap start
csr10000v# monitor capture mycap export tftp://192.168.3.91/mycap.pcap
.!
Exported Successfully

csr10000v#monitor capture mycap stop
```