

IP Observability Devices

1. General Description

The <current Solaris release> now supports the ability to observe packets at the IP layer. Through IP observability devices, the administrator can access all packets with addresses that are associated with [any](#) interface [in the system](#). The addresses include all local addresses as well as addresses that are hosted on non-loopback interfaces and logical interfaces. The observable traffic can be both IPv4 and IPv6 packets.

With IP observability devices, packet flow in zones can be observed. An administrator for a global zone can monitor traffic between zones as well as within a zone. The administrator can observe all loopback IP traffic, traffic from remote machines, packets that are being sent from the system, and forwarded traffic. An administrator of a non-global zone can also observe traffic that is sent and received by that zone.

2. The snoop Command

The snoop utility captures packets from the network and displays the packets' contents. With the introduction of the IP observability devices, a new option, `-I`, has been added to the snoop command. This option directs the command to open the observability device instead of the actual data-link layer device to capture and display packet data.

3. Monitoring IP Traffic

Note — Other procedures that use the snoop command are documented on pp. 193-196 of the System Administration Guide: IP Services.

3.1. Procedure

1. On the local host, assume the Network Management role or become superuser.
Roles contain authorizations and privileged commands. For more information about roles, see "Configuring RBAC (Task Map)" in System Administration Guide: Security Services.
2. If necessary, print information about the interfaces that are attached to the system.
`# ifconfig -a`
3. Type the snoop command to capture the IP traffic on a specific interface.
`# snoop -I <interface> [-V | -v]`

3.2 Examples

The system has the following network device configuration:

```
# ifconfig -a  
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>  
mtu 8232 index 1  
____ inet 127.0.0.1 netmask ff000000
```

```

lo0:1: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>
mtu 8232 index 1
    zone sandbox
    inet 127.0.0.1 netmask fff00000
lo0:2: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>
mtu 8232 index 1
    zone toybox
    inet 127.0.0.1 netmask fff00000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
    inet 129.156.211.94 netmask ffff800 broadcast 129.156.215.255
    ether 8:0:20:f7:d5:79
hme0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
    zone sandbox
    inet 172.0.0.3 netmask fff0000 broadcast 172.0.255.255
hme0:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
    zone toybox
    inet 172.0.0.1 netmask fff0000 broadcast 172.0.255.255
#

```

The output shows three interfaces in the system as follows:

<i>Interfaces</i>	<i>Address</i>	<i>Zone</i>
lo0	127.0.0.1	Global
lo0:1	127.0.0.1	Zone 1 (sandbox)
lo0:2	127.0.0.1	Zone 2 (toybox)
hme0	129.156.211.94	Global
hme0:1	172.0.0.3	Zone 1 (sandbox)
hme0:2	172.0.0.1	Zone 2 (toybox)

The examples show the different output that is generated when you capture packets.

3.2.1 Traffic on the Loopback Interface

```
# snoop -I lo0
```

Using device ipnet/lo0 (promiscuous mode)

```
localhost -> localhost ICMP Echo request (ID: 5550 Sequence number: 0)
```

```
localhost -> localhost ICMP Echo reply (ID: 5550 Sequence number: 0)
```

3.2.2 IPv6 Packet Traffic

```
# snoop -I hme0
Using device ipnet/hme0 (promiscuous mode)
host1 -> host2 TCP D=22 S=62071 Ack=2940511015 Seq=983053346 Len=0
Win=49640
host1 -> host2 TCP D=22 S=62071 Ack=2940511079 Seq=983053346 Len=0
Win=49640
host1 -> host2 TCP D=22 S=35934 Push Ack=3056780267 Seq=1084716001 Len=48
Win=49640
fe80::a00:20ff:fe7:d579 -> fe80::a00:20ff:fe7:d579 ICMPv6 Echo request (ID: 5567
Sequence number: 0)
fe80::a00:20ff:fe7:d579 -> fe80::a00:20ff:fe7:d579 ICMPv6 Echo reply (ID: 5567
Sequence number: 0)
host1 -> host2 TCP D=22 S=35934 Ack=3056780395 Seq=1084716049 Len=0
Win=49640
host1 -> host2 TCP D=22 S=35934 Ack=3056780443 Seq=1084716049 Len=0
Win=49640
```

3.2.3 Packet Flow in the hme0 Device in a Local Zone (Sandbox)

```
# snoop -I hme0 -v port 22
IPNET: ----- IPNET Header -----
IPNET:
IPNET: Packet 5 arrived at 15:16:50.85262
IPNET: Packet size = 64 bytes
IPNET: dli_version = 1
IPNET: dli_type = 0
IPNET: dli_srczone = 0
IPNET: dli_dstzone = 1
IPNET:
IP: ----- IP Header -----
IP:
IP: Version = 4
IP: Header length = 20 bytes
IP: Type of service = 0x00
IP: _____ xxx. .... = 0 (precedence)
IP: _____ ..0 .... = normal delay
IP: _____ .... 0... = normal throughput
IP: _____ .... .0.. = normal reliability
IP: _____ .... .0. = not ECN capable transport
IP: _____ .... ..0 = no ECN congestion experienced
IP: Total length = 40 bytes
IP: Identification = 22629
IP: Flags = 0x4
IP: _____ .1.. .... = do not fragment
IP: _____ ..0. .... = last fragment
```

IP: Fragment offset = 0 bytes
IP: Time to live = 64 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 0000
IP: Source address = 172.0.0.1, 172.0.0.1
IP: Destination address = 172.0.0.3, 172.0.0.3
IP: No options
IP:
TCP: ----- TCP Header -----
TCP:
TCP: Source port = 46919
TCP: Destination port = 22
TCP: Sequence number = 3295338550
TCP: Acknowledgement number = 3295417957
TCP: Data offset = 20 bytes
TCP: Flags = 0x10
TCP: 0... .. = No ECN congestion window reduced
TCP: .0.. .. = No ECN echo
TCP: ..0. = No urgent pointer
TCP: ...1 = Acknowledgement
TCP 0... = No push
TCP0.. = No reset
TCP:0. = No Syn
TCP: 0 = No Fin
TCP: Window = 49152
TCP: Checksum = 0x0014
TCP: Urgent pointer = 0
TCP: No options
TCP:

3.2.4 All Traffic in the hme0 Device in the Global Zone

```
# snoop -I hme0 -c 10
Using device ipnet/hme0 (promiscuous mode)
host1 -> host2 TCP D=22 S=48401 Ack=2300132576 Seq =688720387 Len=0
Win=49640
host1 -> host2 TCP D=22 S=48401 Ack=2300132656 Seq =688720387 Len=0
Win=49640
host1 -> host2 TCP D=22 S=48469 Push Ack=230992952 6 Seq=3030846960 Len=48
Win=49640
 172.0.0.3 -> 172.0.0.1 ICMP Echo request (ID: 6070 Sequence number: 0)
 172.0.0.1 -> 172.0.0.3 ICMP Echo reply (ID: 6070 Sequence number: 0)
host1 -> host2 TCP D=22 S=48469 Ack=2309929638 Seq =3030847008 Len=0
Win=49640
host1 -> host2 TCP D=22 S=48469 Ack=2309929686 Seq =3030847008 Len=0
Win=49640
```

otis -> host2 RPC R XID=1164932699 Success
otis -> host2 RPC R XID=1164932700 Success
otis -> host2 RPC R XID=1164932701 Success
10 packets captured
#