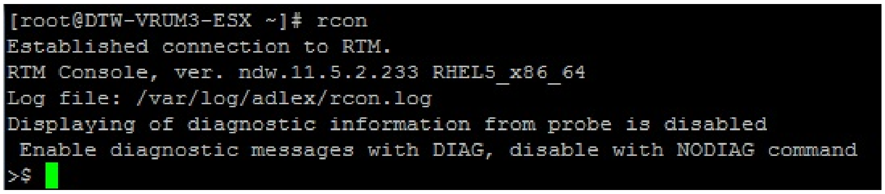
Capturing Packet Traces on AMD

The following instructions and examples are related to capturing packets on AMD.

NOTE: The following commands don't apply to the HS AMD.

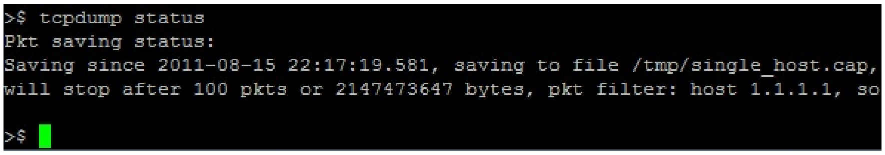
1. How to capture a packet trace on the AMD?

1. In order to be able to use the **tcpdump** utility to capture packets, login to the AMD, type the **rcon** command and press **Enter** at the Linux prompt.



```
[root@DTW-VRUM3-ESX ~]# rcon
Established connection to RTM.
RTM Console, ver. ndw.11.5.2.233 RHEL5_x86_64
Log file: /var/log/adlex/rcon.log
Displaying of diagnostic information from probe is disabled
 Enable diagnostic messages with DIAG, disable with NODIAG command
>$
```

2. Before starting the capture, make sure that there are no other captures already running by executing the **tcpdump status** command.

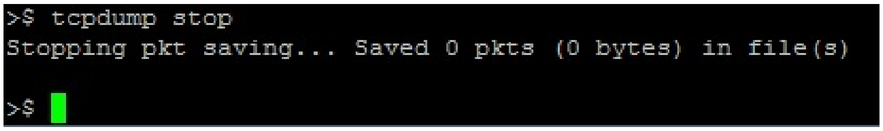


```
>$ tcpdump status
Pkt saving status:
Saving since 2011-08-15 22:17:19.581, saving to file /tmp/single_host.cap,
will stop after 100 pkts or 2147473647 bytes, pkt filter: host 1.1.1.1, so

>$
```

If there's already a capture running (as shown above), you need to stop it before starting a new one. To do that, execute the **tcpdump stop** command.

Note that the **tcpdump stop** command is also used to stop and save the trace file after you are satisfied with the amount of data captured.



```
>$ tcpdump stop
Stopping pkt saving... Saved 0 pkts (0 bytes) in file(s)

>$
```

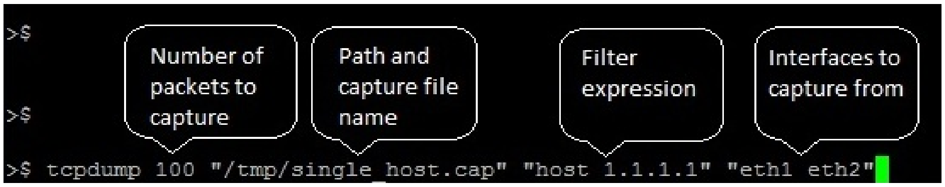
Syntax:

Number of packets to capture: This can be any number of packets between 1 and 2808348672. Setting this value to "0", will keep on capturing packets until you execute **tcpdump stop**, 2808348672 packets or 2147473647 bytes are collected.

Path and capture file name: This should be the path-to and name-of your trace file. This field should be enclosed in double-quotes ("").

Filter expression: This is the expression to be used by the **tcpdump** utility only to capture packets that meet your criteria. This field should be enclosed in double-quotes (""). More information on this filter expression is provided in the "Examples" section below.

Interfaces to capture from (optional): This is an optional field and when it is omitted, the AMD will capture traffic using your filter expression from all the interfaces that are configured as sniffing. This field should be enclosed in double-quotes ("").



Number of packets to capture
Path and capture file name
Filter expression
Interfaces to capture from

```
>$

>$

>$ tcpdump 100 "/tmp/single_host.cap" "host 1.1.1.1" "eth1 eth2"
```

Examples:

Capturing 100 packets from a single host:
tcpdump 100 "/tmp/single_host.cap" "host 1.1.1.1"

On This Page

1. How to capture a packet trace on the AMD?
2. How to schedule traffic capturing using the tcpdump command?

Related Pages

Capturing Packets on AMD

Smart Packet Capture

TCPDUMP

Capturing 100 packets from a single host and tcp port 80:

```
tcpdump 100 "/tmp/single_host_port.cap" "host 1.1.1.1 and port 80"
```

Capturing packets for multiple hosts without a preset packet limit:

```
tcpdump 0 "/tmp/mulit_host.cap" "host 1.1.1.1 or host 2.2.2.2 or host 3.3.3.3"
```

Capturing 100 packets for a single host on a specific interface:

```
tcpdump 100 "/tmp/host_ifc.cap" "host 1.1.1.1" "eth2"
```

Capturing 100 packets for a subnet on a specific interface:

```
tcpdump 100 "/tmp/sub_ifc.cap" "net 1.1.1.1/11" "eth3"
```

Capturing traffic with VLAN tags for a specific host:

```
tcpdump 0 "/tmp/vlan_host.cap" "vlan and host 1.1.1.1"
```

Capturing traffic with regular Ethernet frames or VLAN tagged frames for a specific host:

```
tcpdump 0 "/tmp/vlan_host.cap" "(host 1.1.1.1) or (vlan and host 1.1.1.1)"
```

Capturing traffic with MPLS tags for a specific host:

```
tcpdump 0 "/tmp/vlan_host.cap" "mpls and host 1.1.1.1"
```

Capturing traffic with regular Ethernet frames, VLAN or MPLS tagged frames for a specific host:

```
tcpdump 0 "/tmp/vlan_host.cap" "(host 1.1.1.1) or (vlan and host 1.1.1.1) or (mpls and host 1.1.1.1)"
```

2. How to schedule traffic capturing using the tcpdump command?

If you need to schedule traffic capturing using the rcon's **tcpdump** command, add the following lines to the AMD's **/etc/crontab** file (in case of compatibility issues, please refer to the given crontab syntax):

```
0 18 11 * * root /usr/adlex/rtm/bin/rcmd -c' ' 'tcpdump 0 "/var/tmp/nightly.pcap" "host x.x.x.x"'
0 */1 11,12 * * root /usr/adlex/rtm/bin/rcmd -c' ' 'tcpdump status' >> /var/tmp/nightly.log #optional line, generating "log file" hourly
0 6 12 * * root /usr/adlex/rtm/bin/rcmd -c' ' 'tcpdump stop'
```

The above example will result in capturing the traffic between 6:00 PM every 11th day of each month and 6:00 AM evary 12th day of each month. Meanwhile, the log file will be supplemented every hour.

Note: It's crucial to use the following syntax:
rcmd -c' ' 'tcpdump ......'