



# Ethalyzer

This chapter describes how to use Ethalyzer as a Cisco NX-OS protocol analyzer tool.

## Information About Ethalyzer

Ethalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethalyzer is a command-line version of Wireshark that captures and decodes packets. You can use Ethalyzer to troubleshoot your network and analyze the control-plane traffic.

To configure Ethalyzer, use one or more of the following commands.

Command	Purpose
<code>ethalyzer local interface <i>interface</i></code>	Captures packets sent or received by the supervisor and provides detailed protocol information. <b>Note</b> For all commands in this table, the interface is control, ha-primary, ha-secondary, inband (packet interface) or mgmt (management interface).
<code>ethalyzer local interface <i>interface</i> limit-captured-frames</code>	Limits the number of frames to capture.
<code>ethalyzer local interface <i>interface</i> limit-frame-size</code>	Limits the length of the frame to capture.
<code>ethalyzer local interface <i>interface</i> capture-filter</code>	Filters the types of packets to capture.
<code>ethalyzer local interface <i>interface</i> display-filter</code>	Filters the types of captured packets to display.
<code>ethalyzer local interface <i>interface</i> raw</code>	Dump the packet in HEX/ASCII with a one line summary.
<code>ethalyzer local interface <i>interface</i> write</code>	Saves the captured data to a file.
<code>ethalyzer local read file</code>	Opens a captured data file and analyzes it.

Ethalyzer does not capture data traffic that Cisco NX-OS forwards in the hardware. Ethalyzer uses the same capture filter syntax as tcpdump. For more information, see the following URL:

[http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)

For information about the syntax of the display filter, see the following URL:

<http://wiki.wireshark.org/DisplayFilters>

This example shows captured data (limited to four packets) on the management interface:

```
switch# ethalyzer local interface mgmt limit-captured-frames 4
Capturing on eth1
2012-10-01 19:15:23.794943 10.78.110.241 -> 72.163.145.51 SSH Encrypted response packet
len=64
2012-10-01 19:15:23.796142 10.78.110.241 -> 72.163.145.51 SSH Encrypted response packet
len=144
2012-10-01 19:15:23.796608 10.78.110.241 -> 72.163.145.51 SSH Encrypted response packet
len=144
2012-10-01 19:15:23.797060 10.78.110.241 -> 72.163.145.51 SSH Encrypted response packet
len=144
4 packets captured
switch#
```

For information about Wireshark, see the following URL: <http://www.wireshark.org/docs/>