Ethanalyzer

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

This chapter includes the following section:

Using Ethanalyzer

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

To configure Ethanalyzer, use one or more of the following commands:

Table 27-1 Ethanalyzer Commands Used for Configuring

Command	Purpose
switch# **ethanalyzer local sniff-interface** *interface*	Captures packets sent or received by the supervisor and provides detailed protocol information. **Note** For all commands in this table, interface is control, ha-primary, ha-secondary, inband (packet interface) or mgmt (management interface).
switch# **ethanalyzer local sniff-interface** *interface* **detailed-dissection**	Displays detailed protocol information
switch# **ethanalyzer local sniff-interface** *interface* **limit-captured-frames**	Limits the number of frames to capture.
switch# **ethanalyzer local sniff-interface** *interface* **limit-frame-size**	Limits the length of the frame to capture.
switch# **ethanalyzer local sniff-interface** *interface* **capture-filter**	Filters the types of packets to capture.
switch# **ethanalyzer local sniff-interface** *interface* **display-filter**	Filters the types of captured packets to display.
switch# **ethanalyzer local sniff-interface** *interface* **dump-pkt**	Dump the packet in HEX/ASCII with possibly one line summary

Table 27-1 Ethanalyzer Commands Used for Configuring

Command	Purpose
switch# **ethanalyzer local sniff-interface** *interface* **write**	Saves the captured data to a file.
switch# **ethanalyzer local read file**	Opens a captured data file and analyzes it.

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

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# ethanalyzer local sniff-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 more information about Wireshark, see the following URL: http://www.wireshark.org/docs/