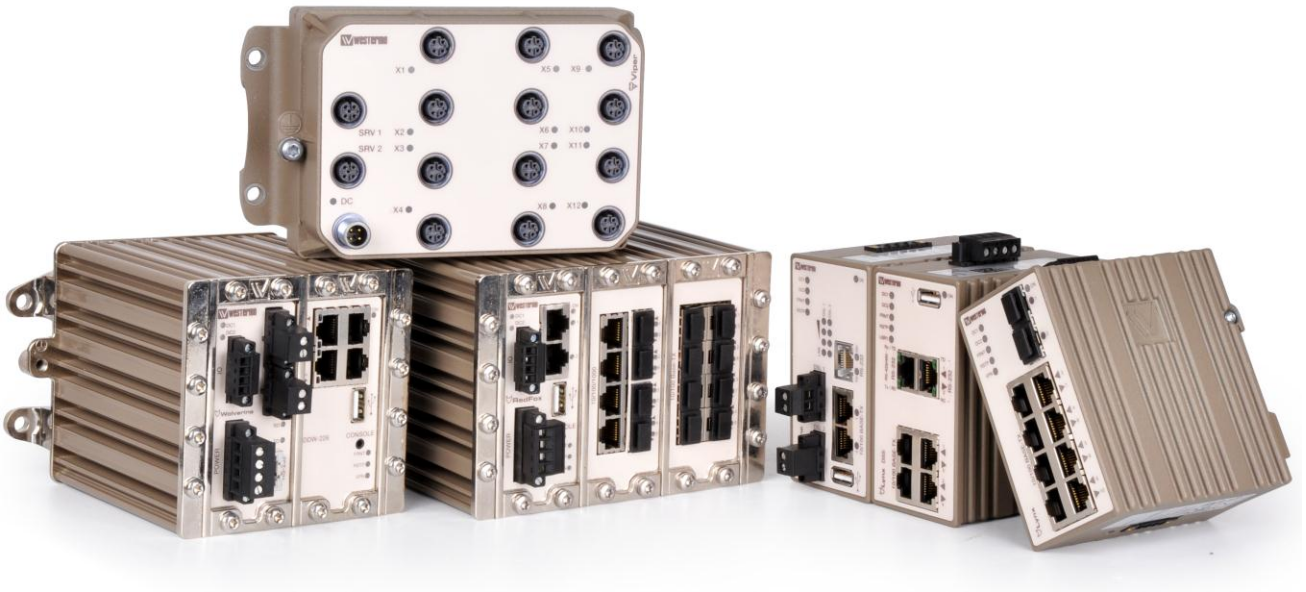
TECH NOTE

WeOS Tcpdump

Manage the built-in packet sniffer



Background

Packet sniffer that by default prints the header of each packet captured.

Note:
Only routed traffic, or traffic destined for the device itself, is possible to capture with this tool. Hence, switched Layer-2 traffic is not visible.

WeOS Tcpdump syntax

tcpdump [[iface] <IFNAME>] [...] [expr <FILTER>]

Example: tcpdump vlan1

WeOS Tcpdump options

count <NUMBER>
Exit after receiving *count* number of packets.

Example: tcpdump vlan1 count 10

in <URI://path/to/file.pcap>
Read a saved pcap file. Only USB storage at the moment.

Example: tcpdump in usb://log/vlan1.pcap

out <URI://path/to/file.pcap>
Write a pcap file. Only USB storage at the moment.

Example: tcpdump vlan1 out usb://log/vlan1.pcap

snaplen <BYTES>
Snarf *snaplen* bytes of data from each packet rather than the default of 68 bytes. Packets truncated because of a limited snapshot are indicated in the output with "[|proto]", where proto is the name of the protocol level at which the truncation has occurred.

Example: tcpdump vlan1 snaplen 1522
Example: tcpdump vlan1 snaplen 45

16:23:14.259531 arp reply 192.168.2.202 is-at 00:07:7c:0a:a8:41
16:23:14.237021 IP 192.168.2.69.7905 > 192.168.2.202.http: [|tcp]

hex

When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII.

Example: tcpdump vlan1 hex

```
17:22:29.590422 arp who-has 192.168.2.202 tell 192.168.2.69
        0x0000   ffff ffff ffff 9c8e 993d 0196 0806 0001          .........=......
        0x0010   0800 0604 0001 9c8e 993d 0196 c0a8 0245          .........=.....E
        0x0020   0000 0000 0000 c0a8 02ca 0000 0000 0000          ................
        0x0030   0000 0000 0000 0000 0000 0000 882a               .............*
17:22:29.610567 arp reply 192.168.2.202 is-at 00:07:7c:0a:a8:41
        0x0000   9c8e 993d 0196 0007 7c0a a841 0806 0001          ...=....|..A....
        0x0010   0800 0604 0002 0007 7c0a a841 c0a8 02ca          ........|..A....
        0x0020   9c8e 993d 0196 c0a8 0245                         ...=.....E
```

numeric

Do not convert addresses to names (i.e host addresses, port numbers etc).

verbose

When parsing and printing, produce (slightly more) verbose output.
For example, the time to live, identification, total length and options in an IP packet are printed.

Example: ssh packet non verbose:

15:10:51.098824 IP 192.168.2.69.5392 > 192.168.2.202.ssh: S 1730388179:1730388179(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>

Example: ssh packet verbose:

15:08:38.911630 IP *(tos 0x0, ttl 128, id 7912, offset 0, flags [DF], length: 52)* 192.168.2.69.5217 > 192.168.2.202.ssh: S *[tcp sum ok]* 2508578149:2508578149(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>

WeOS Tcpdump filter

expr ”<FILTER>”

selects which packets will be dumped. If no *expression* is given, all packets on the net will be dumped.
Otherwise, only packets for which *expression* is `true' will be dumped, this is not a display filter.
Remeber to put the filter within quotation marks.

For more filtering information visit:
http://www.wireshark.org/docs/man-pages/pcap-filter.html

Tcpdump Primitives

Direction Primitives

dst		Ex: tcpdump vlan1 expr “dst 192.168.2.202”
src		Ex: tcpdump vlan1 expr ”src 192.168.2.69”
	net	Ex: tcpdump vlan1 expr “src net 192.168.2.0/24”
	port	Ex: tcpdump vlan1 expr “dst port 22”

Protocol primitives

icmp, **igmp**, **esp**, **vrrp**, **udp**, **tcp**, **ip**, **ether**, **arp** etc.
Ex: tcpdump vlan1 expr ”vrrp”
Ex: tcpdump vlan1 expr "ether dst 00:07:7c:0a:a8:41"

Multicast primitive

multicast	Ex: tcpdump vlan1 expr ”multicast"

Tcpdump Filter Operators

!	Ex: tcpdump vlan1 expr “!port 22”
not	Ex: tcpdump vlan1 expr “not port 22”
&&	Ex: tcpdump vlan1 expr “dst 192.168.2.202 && port 22”
and	Ex: tcpdump vlan1 expr “dst 192.168.2.202 and port 22”
||	Ex: tcpdump vlan1 expr “port 80 || port 22”
or	Ex: tcpdump vlan1 expr “port 80 or port 22”

Revision history for version 1.0

Revision	Rev by	Revision note	Date
00	ML	First version	2014-03-09
01	ML	Changed type to TechNote	2014-04-25
02			
03			
04			
05			
06			
07			

HEAD OFFICE

Sweden
Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units
Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.