Ubuntu Manpage:

horst

bionic (8) horst.8.gz

Provided by: horst_5.0-2_amd64

NAME

horst - Highly Optimized Radio Scanning Tool

SYNOPSIS

horst [**-v**] [**-h**] [**-q**] [**-D**] [**-a**] [**-c** file] [**-C** channel] [**-i** interface] [**-t** sec] [**-V** view]
[**-d** ms] [**-b** bytes] [**-M** file] [**-s**] [**-u**] [**-N**] [**-n** IP] [**-p** port] [**-o** file] [**-X** name] [**-x**
command] [**-e** mac] [**-f** pkt_name] [**-m** mode] [**-B** BSSID]

DESCRIPTION

horst is a small, lightweight IEEE802.11 wireless LAN analyzer with a text interface. Its
basic function is similar to tcpdump, Wireshark or Kismet, but it's much smaller and shows
different, aggregated information which is not easily available from other tools. It is
mainly targeted at debugging wireless LANs with a focus on ad-hoc (IBSS) mode in larger
mesh networks. It can be useful to get a quick overview of what's going on on all wireless
LAN channels and to identify problems.

· Shows signal values per station.

· Calculates channel utilization ("usage") by adding up the amount of time the packets
actually occupy the medium.

· "Spectrum Analyzer" shows signal levels and usage per channel.

· Text-based "graphical" packet history, with signal, packet type and physical rate

· Shows all stations per ESSID and the live TSF per node as it is counting.

· Detects IBSS "splits" (same ESSID but different BSSID - this is a common driver

problem).

· Statistics of packets/bytes per physical rate and per packet type.

· Has some support for mesh protocols (OLSR and batman).

· Can filter specific packet types, source MAC addresses or BSSIDs.

· Client/server support for monitoring on remote nodes.

· Can be controlled via a named pipe.

See MONITOR MODE below for more information about the network interface setup.

OPTIONS

-v Show version.

-h Show summary of options.

-q Quiet mode. Don't show user interface. This is only useful in conjunction when
running in server mode (-C) or writing to a file (-o).

-D Show lot's of debugging output, including a full package dump. Only available when
compiled with DEBUG=1.

-a Always add virtual monitor interface. Don't try to set existing interface to
monitor mode.

-c configfile
Use configfile instead of the default "/etc/horst.conf".

-C channel
Set inital channel (number not frequency).

-i intf
Operate on the given network interface instead of the default "wlan0".

-t sec Timeout (remove) nodes after not receiving packets from them for this time in
seconds (default: 60 sec).

-V view
Display 'view'. Valid view names are "history", "hist", "essid", "statistics",
"stats", "spectrum", "spec".

-d ms Display update interval. The default value of 100ms can be increased to reduce CPU
load caused by redrawing the screen.

-b bytes
Receive buffer size. The receive buffer size can be set to tune memory consumption
and reduce lost packets under load.

-M filename
MAC address to host name mapping file. The file can either be a dhcp.leases file
from dnsmasq or contain mappings in the form "MAC<space>name" (e.g.:
"00:01:02:03:04:05 test") line by line (default filename: /tmp/dhcp.leases).

-s Show a poor mans "spectrum analyzer". The same can be achieved by running **horst** as
normal and pressing the button 's' (Spec); then 'c' (Chan) and 'a' (Automatically
change channel).

-u Upper channel limit for the automatic channel change.

-N Allow client connections. Server mode. Only one client connection is supported at
the moment (default: off).

-n IP Connect to a **horst** instance running in server-mode at the specified IP address.

-p port
Use the specified port (default: 4444) for client/server connections.

-o filename
Write a information about each received packet into file. Note that you can send to
STDOUT by using **-o /dev/stdout**. See OUTPUT FILE FORMAT below.

-X Accept control commands on a named pipe (default /tmp/horst).

-X name
Accept control commands on a named pipe with given name or set pipe name used with
-x.

-x command
Send control command to another **horst** process who was started with -X and then
exit. Multiple commands can be concatenated with ';'. Currently implemented
commands are:

pause
Pause **horst** processing

resume
Resume **horst** processing

reset
Reset all history, statistics and views

channel=X
Set channel channel number

channel_scan=X
Automatically change channels (1 or 0)

channel_dwell=X
Set channel dwell time when automatically changing channel (ms)

channel_upper=X
Set max channel when automatically changing channel

outfile=X
Write to outfile named X. If the file is already open, it is cleared and re-openend. If filename is not specified ("outfile=") any existing file is closed and no file is written.

-e MAC Filter all MAC addresses except these, to show only packets originating from the
specified MAC addresses. This option can be specified multiple times.

-f pkt_type
Filter all packets except these. This option can be specified multiple times. For
valid packet names see NAMES AND ABBREVIATIONS below.

-m (AP|STA|ADH|PRB|WDS|UNKNOWN)
Only show/include packets and nodes of this mode. Note that the mode is infered by
the information of packets we received and it may take some time until a node is
properly classified. This option can be specified multiple times.

-B BSSID
Only show/include packets which belong to the given BSSID.

TEXT USER INTERFACE

The ncurses-based text interface tries to display a lot of information, so it may look
confusing at first. Below we describe the different screens and options.

Main screen

The initial (main) screen is split into three parts. The upper area shows a list of
aggregated "node" information, the most useful information about each sender which
was discovered, one per line:

/
"Spinner" to show activity

Pk
Percentage of this node's packets in relation to all received packets

Re%
Percentage of retried frames of all frames this node sent

Cha
Channel number

Sig
Signal value (RSSI) in dBm

RAT
Physical data rate

TRANSMITTER

MAC address of sender

MODE
Operating Mode (AP, AHD, PRB, STA, WDS), see "NAMES AND ABBREVIATIONS"

ENCR
Encryption (WPA1, WPA2, WEP)

ESSID
ESSID

INFO
Additional info like "BATMAN", IP address...

The lower area shows a scrolling list of packets as they come in:

Cha
Channel number

Sig
Signal value (RSSI) in dBm

RAT
Physical data rate

TRANSMITTER
MAC address of sender

BSSID
BSSID

TYPE
Packet type, see "NAMES AND ABBREVIATIONS"

INFO
Additional info like ESSID, TFS, IP address...

The lower right box shows bar graphs for:

Signal of last received packet in green

bps Bits per second of all received packets

Usage Percentage of channel use

The lower edge is the menu and status bar, it shows which keys to press for other
screens. The status shows ">" when **horst** is running or "=" when it is paused, then
"F" when any kind of filter is active, the Channel, the monitor interface in use
and the time.

Pause ('p' or <space>)

Can be used to pause/resume **horst**. When **horst** is paused it will loose packets
received in the mean time.

Reset ('r')

Clears all history and aggregated statistical data.

History ('h')

The history screen scrolls from right to left and shows a bar for each packet
indicating the signal level. In the line below that, the packet type is indicated
by one character (See NAMES AND ABBREVIATIONS below) and the rough physical data
rate is indicated below that in blue.

ESSID ('e')

The ESSID screen groups information by ESSID and shows the mode (AP, IBSS), the MAC
address of the sender, the BSSID, the TSF, the beacon interval, the channel, the
signal, a "W" when encrytoion is used and the IP address if known.

Statistics ('a')

The statistics screen groups packets by physical rate and by packet type and shows
other kinds of aggregated and statistical information based on packets.

Spectrum Analyzer ('s')

The "poor mans spectrum analyzer" screen is only really useful when **horst** is
started with the -s option or the "Automatically change channel" option is selected
in the "Chan" settings, or the config option channel_scan is set.

It shows the available channels horizontally and vertical bars for each channel:

Signal in green

Physical rate in blue

Channel usage in orange/brown

By pressing the 'n' key, the display can be changed to show only the average signal level
on each channel and the last 4 digits of the MAC address of the individual nodes at the
level (height) they were received. This can give a quick graphical overview of the

distance of nodes.

Filters ('f')

This configuration dialog can be used to define the active filters.

Channel Settings ('c')

This configuration dialog can be used to change the channel changing behaviour of
horst or to change to a different channel manually.

Sort ('o')

Only active in the main screen, can be used to sort the node list in the upper area
by Signal, Time, BSSID or Channel.

NAMES AND ABBREVIATIONS

802.11 standard frames

Management frames

a	ASOCRQ	Association request
A	ASOCRP	Associaion response
a	REASRQ	Reassociation request
A	REASRP	Reassociation response
p	PROBRQ	Probe request
P	PROBRP	Probe response
T	TIMING	Timing Advertisement
B	BEACON	Beacon
t	ATIM	ATIM
D	DISASC	Disassociation
u	AUTH	Authentication
U	DEAUTH	Deauthentication
C	ACTION	Action

c | ACTNOA | Action No Ack

Control frames

w	CTWRAP	Control Wrapper
b	BACKRQ	Block Ack Request
B	BACK	Block Ack
s	PSPOLL	PS-Poll
R	RTS	RTS
C	CTS	CTS
K	ACK	ACK
f	CFEND	CF-End
f	CFENDK	CF-End + CF-Ack

Data frames

D	DATA	Data
F	DCFACK	Data + CF-Ack
F	DCFPLL	Data + CF-Poll
F	DCFKPL	Data + CF-Ack + CF-Poll
n	NULL	Null (no data)
f	CFACK	CF-Ack (no data)
f	CFPOLL	CF-Poll (no data)
f	CFCKPL	CF-Ack + CF-Poll (no data)
Q	QDATA	QoS Data
F	QDCFCK	QoS Data + CF-Ack
F	QDCFPL	QoS Data + CF-Poll
F	QDCFKP	QoS Data + CF-Ack + CF-Poll
N	QDNULL	QoS Null (no data)
f	QCFPLL	QoS CF-Poll (no data)
f	QCFKPL	QoS CF-Ack + CF-Poll (no data)
*	BADFCS	Bad frame checksum

Packet types

Similar to 802.11 frames above but higher level and as a bit field (types can

overlap, e.g. DATA + IP) and including more information, like IP, ARP, BATMAN,

OLSR...

Packet types

CTRL	0x000001	WLAN Control frame
MGMT	0x000002	WLAN Management frame
DATA	0x000004	WLAN Data frame
BADFCS	0x000008	WLAN frame checksum (FCS) bad
BEACON	0x000010	WLAN beacon frame
PROBE	0x000020	WLAN probe request or response
ASSOC	0x000040	WLAN associaction request/response frame
AUTH	0x000080	WLAN authentication frame
RTSCTS	0x000100	WLAN RTS or CTS
ACK	0x000200	WLAN ACK or BlockACK
NULL	0x000400	WLAN NULL Data frame
QDATA	0x000800	WLAN QoS Data frame (WME/WMM)
ARP	0x001000	ARP packet
IP	0x002000	IP packet
ICMP	0x004000	IP ICMP packet
UDP	0x008000	IP UDP
TCP	0x010000	IP TCP
OLSR	0x020000	OLSR protocol
BATMAN	0x040000	BATMAND Layer3 or BATMAN-ADV Layer 2 frame
MESHZ	0x080000	MeshCruzer protocol

Operating modes

Bit field of operating mode type which is infered from received packets. Modes may
overlap, i.e. it is common to see STA and PRB at the same time.

Operating modes

AP | 0x01 | Access Point (AP)
ADH | 0x02 | Ad-hoc node

STA | 0x04 | Station (AP client)
PRB | 0x08 | Sent PROBE requests
WDS | 0x10 | WDS or 4 Address frames
UNKNOWN | 0x20 | Unknown e.g. RTS/CTS or ACK

MONITOR MODE

To capture and analyze 802.11 traffic, the interface needs to be in monitor mode. You can
either setup the interface manually beforehand or let **horst** setup it automatically at
startup. Usually, root privileges are required to modify an interface setup.

horst should work with any wireless LAN card and driver which supports monitor mode, with
either "prism2" or "radiotap" headers. This includes most modern mac80211-based drivers.

If the interface is not in monitor mode at startup, **horst** first tries to put the interface
in monitor mode. If it fails (for example when the interface is already in use), a new
virtual monitor interface (horst0) is added and used instead. The virtual monitor
interface is removed when **horst** exits. Note that changing the channel via a virtual
monitor interface is not allowed by the wireless driver, so options -C and -s do not work
when virtual monitor interface is used.

Examples of how to setup an interface manually:

Using iw:
iw wlan0 interface add mon0 type monitor

or

sudo iw wlan1 set type monitor
sudo iw wlan1 set channel 6

Using iwconfig:
iwconfig wlan0 mode monitor
iwconfig wlan0 channel 1
ifconfig wlan0 up

Using madwifi:
wlanconfig wlan0 create wlandev wifi0 wlanmode monitor

Using hostap:
iwconfig wlan0 mode monitor
iwpriv wlan0 monitor_type 1

NOTES

Signal values and ranges may differ between wireless drivers and versions.

OUTPUT FILE FORMAT

The format of the output file (-o flag) is a comma separated list of the following fields
in the following order, one packet each line.

timestamp
Local time, including microseconds (e.g. 2015-05-16 15:05:44.338806 +0300)

packet_type
802.11 MAC packet type name as defined in the section "NAMES AND ABBREVIATIONS".

wlan_src
Source MAC address

wlan_dst
Destination MAC address

wlan_bssid
BSSID

pkt_types
Higher level packet name as defined in section "NAMES AND ABBREVIATIONS".

phy_signal
Signal strength in dBm

wlan_len
Packet length (MAC)

phy_rate
Physical data rate

phy_freq
Received while tuned to this frequency.

wlan_tsf
TFS timer value

wlan_essid
ESSID, network name

wlan_mode
Operating modes as defined in "NAMES AND ABBREVIATIONS".

wlan_channel
Channel number

wlan_wep
Encryption in use

wlan_wpa
WPA1 Encryption in use

wlan_rsn
RSN (WPA2) Encryption in use

ip_src IP source address (if available)

ip_dst IP destionation address (if available)

SEE ALSO

horst.conf(5), tcpdump(1), wireshark(1), kismet(1), **README,** http://br1.einfach.org/tech/horst

horst was written by Bruno Randolf <br1@einfach.org>.

This manual page was written by Antoine Beaupré <anarcat@debian.org>, for the Debian project (and may be used by others).

July 22, 2015 HORST(8)