APRECV

Section: User Commands (1)
Index Return to Main Contents

NAME

APRecv - Network testing tool to recieve arbitrary packets

SYNOPSIS

aprecv [Options]

DESCRIPTION

APRecv is designed to receive arbitrary network packets and print out the protocols. *APRecv* supports many protcols, look at *PROTOCOLS* for a list of all. Many options like bpf filter or checking the IP checksum are also given, see *OPTIONS* section for more details. Some protocols contains strings to print out, for example PAP, if the string contains non-printable characters a "." is filled in.

OPTIONS

--calc-checksums
: Calculate the checksums of the protocols(currently IP and ICMPv4 implemented) and print the correct if wrong.

--check-for-errors
: Check the packets for errors and print them out. If --statistic is used the errors will counted and print them with the statistics.

-c | --count
: Count all bytes *APRecv* recieved.

-d | --device <device>
: Here you specify the device to use *APRecv* should use to receive.

-D | --daemon
: Run *APRecv* in daemon mode, fork in background and exit.

--expand-<protocol>
: Expand the protocol header. Following options are available --expand-all, --expand-ethernet, --expand-arp and --expand-pppoe.

-f | --filter filter rule
: Set up a bpf filter rule.

-F -filter filter rule
: Set up a bpf filter rule, not optimized.

-h | -?
: Display a help message and exit.

-l | --logfile <file>
Log all informations about packets which are normally printed to stdout in a file. If the file exists, *APRecv* add the new informations, otherwise it create a new.

--max-packets <num>
Maximum packets to receive, default is a loop.

--print-<protocol>-hex
Print the payload of an packet in hex. Following options are available --print-ip-hex, --print-pppoe-hex, --print-tcp-hex and --print-udp-hex.

--print-<protocol>-text
Print the payload of packet in text. Following options are available --print-tcp-text and --print-udp-text.

-p | --promisc <0|1>
Enable or disable promisc mode for the device if on(1) or off(2) is specified. Promisc mode is usefull in ethernet networks to receive packets which are not for the host you work on. It enable the device to receive packets which are not for the mac address of the device.

-P | --pcap-file <file>
Read a raw pcap dump from file.

-r | --logfile-raw <file>
Log all packets in raw in a file.

-R | --print-raw-hex
Print raw packet in hex.

-s | --snaplen <up to 65535>
Set the snaplen for pcap, default is 65535.

--statistic
Print out a statistic about all counted packets and protocols after exiting.

-v | --verbose
Verbose mode print out more informations about the protocols, the interface localnet and netmask address, resolve IP and MAC addresses.

-V | --version
Display the version.

PROTOCOLS

Currently these protocols are supported: Ethernet II, 802.3, 802.2, 802.1p/1q, SNAP, PPPoE with Tags, PPP with LCP, IPCP, IPXCP, ATCP, ECP, PAP and CHAP, ARP/RevARP/InvARP, IPv4/IPv6, IPX, ICMPv4/ICMPv6, IGMP, TCP, UDP, SPX/SPX2, IPComp, IPAuth, SCTP, EGP, GGP, OSPFv2/OSPFv3, NARP, IGRP, RIPv1/RIPv2 and IPXRIP.

SEE ALSO

apsend (1), for bpf filter logic look at libpcap on http://www.tcpdump.org or pcap (3)

AUTHOR

APSR development team, look at http://www.aa-security.de.

REPORTING BUGS

Report bugs to <bugs@aa-security.de>.

Index

NAME
SYNOPSIS
DESCRIPTION
OPTIONS
PROTOCOLS
SEE ALSO
AUTHOR
REPORTING BUGS

This document was created by man2html, using the manual pages.
Time: 05:22:27 GMT, April 21, 2002