Ebtables 使用手册

SYNOPSIS

ebtables[-ttable]-[ACDI]chainrulespecification[matchextensions][watcherextensions]target

ebtables[-ttable]-PchainACCEPT|DROP|RETURN

ebtables[-ttable]-F[chain]

ebtables[-ttable]-Z[chain]

ebtables[-ttable]-L[-Z][chain][[--Ln]|[--Lx]][--Lc][--Lmac2]

ebtables[-ttable]-Nchain[-PACCEPT|DROP|RETURN]

ebtables[-ttable]-X[chain]

ebtables[-ttable]-Eold-chain-namenew-chain-name

ebtables[-ttable]--init-table

ebtables[-ttable][--atomic-filefile]--atomic-commit

ebtables[-ttable][--atomic-filefile]--atomic-init

ebtables[-ttable][--atomic-filefile]--atomic-save

DESCRIPTION

ebtablesisanapplicationprogramusedtosetupandmaintainthetablesofrules(insidetheLinuxkernel)thatinspectEthernetframes.Itisanalogoustothe

iptablesapplication, butlesscomplicated, duetothefactthattheEthernetpro
tocolismuchsimplerthantheIPprotocol.

CHAINS

Therearethreeebtablestableswithbuilt-inchainsintheLinuxkernel. The
setablesareusedtodividefunctionalityintodifferentsetsofrules. Eachseto
frulesiscalledachain. EachchainisanorderedlistofrulesthatcanmatchEther
netframes. IfarulematchesanEthernetframe, thenaprocessingspecificationt
ellswhattodowiththatmatchingframe. Theprocessingspecificationiscalleda
'target'. However, iftheframedoesnotmatchthecurrentruleinthechain, thent
henextruleinthechainisexaminedandsoforth. Theusercancreatenew(user-def
ined)chainsthatcanbeusedasthe'target'ofarule. User-definedchainsarever
yusefultogetbetterperformanceoverthelineartraversaloftherulesandareal
soessentialforstructuringthefilteringrulesintowell-organizedandmainta
inablesetsofrules.

TARGETS

AfirewallrulespecifiescriteriaforanEthernetframeandaframeprocessi
ngspecificationcalledatarget. Whenaframematchesarule, thenthenextaction
performedbythekernelisspecifiedbythetarget. Thetargetcanbeoneofthiseva
lues:ACCEPT, DROP, CONTINUE, RETURN, an'extension'(seebelow)orajumptoause
r-definedchain.

ACCEPTmeanstolettheframethrough. DROPmeanstheframehastobedropped. I
ntheBROUTINGchainhowever, theACCEPTandDROPtargethavedifferentmeanings(
seetheinfoprovidedforthe-toption). CONTINUEmeansthenextrulehastobechec
ked. Thiscanbehandy, f.e., toknowhowmanyframespassacertainpointinthechai
n, tologthoseframesortoapplymultipletargetsonaframe. RETURNmeansstoptra
versingthischainandresumeatthenextruleintheprevious(calling)chain. For

theextensiontargetspleaserefertotheTARGETEXTENSIONSsectionofthismanpage.

TABLES

Asstatedearlier, therearethreeebtablestablesintheLinuxkernel. Thetablenamesarefilter, natandbroute. Ofthesethreetables, thefiltertableisthe defaulttablethatthecommandoperateson. Ifyouareworkingwiththefiltertable, thenyoucandropthe'-tfilter'argumenttotheebtablescommand. However, you willneedtoprovidethe-targumentfortheothertwotables. Moreover, the-targu mentmustbethefirstargumentontheebtablescommandline, ifused.

-t, --table

filteristhedefaulttableandcontainsthreebuilt-inchains:INPUT(forfr amesdestinedforthebridgeitself, ontheleveloftheMACdestinationaddress), OUTPUT(forlocally-generatedor(b)routedframes)andFORWARD(forframesbein gforwardedbythebridge).

natismostlyusedtochangethemacaddressesandcontainsthreebuilt-incha ins:PREROUTING(foralteringframesassoonastheycomein), OUTPUT(foralterin glocallygeneratedor(b)routedframesbeforetheyarebridged)andPOSTROUTING (foralteringframesastheyareabouttogoout). Asmallnoteonthenamingofchain sPREROUTINGandPOSTROUTING:itwouldbemoreaccuratetocallthemPREFORWARDIN GandPOSTFORWARDING, butforallthosewhocomefromtheiptablesworldtoebtable sitiseasiertohavethesamenames. Notethatyoucanchangethename(-E)ifyoudon 'tlikethedefault.

brouteisusedtomakeabrouter, ithasonebuilt-inchain:BROUTING. Thetarg etsDROPandACCEPThaveaspecialmeaninginthebroutetable(thesenamesareused insteadofmoredescriptivenamestokeeptheimplementationgeneric). DROPactu allymeanstheframehastoberouted, whileACCEPTmeanstheframehastobebridged

. The BROUTING chain is traversed very early. However, it is only traversed by frames entering on a bridge port that is in forwarding state. Normally those frames would be bridged, but you can decide otherwise here. The redirect target is very handy here.

EBTABLES COMMAND LINE ARGUMENTS

After the initial ebtables '-t table' command line argument, the remaining arguments can be divided into several groups. These groups are commands, miscellaneous commands, rule specifications, match extensions, watcher extensions and target extensions.

COMMANDS

The ebtables command arguments specify the actions to perform on the table defined with the -t argument. If you do not use the -t argument to name a table, the commands apply to the default filter table. Only one command may be used on the command line at a time, except when the commands -L and -Z are combined, the commands -N and -P are combined, or when --atomic-file is used.

-A, --append

Append a rule to the end of the selected chain.

-D, --delete

Delete the specified rule or rules from the selected chain. There are two ways to use this command. The first is by specifying an interval of rule numbers to delete (directly after -D). Syntax: start_nr[:end_nr] (use -L --Ln to list the rules with their rule number). When end_nr is omitted, all rules starting from start_nr are deleted. Using negative numbers is allowed, for more details about using negative numbers, see the -I command. The second usage is by specifying the complete rule as it would have been specified when it was added. Only the first encountered rule t

hatisthesameasthisspecifiedrule,inotherwordsthematchingrulewiththelow
est(positive)rulenumber,isdeleted.

-C,--change-counters

Changethecountersofthespecifiedruleorrulesfromtheselectedchain.Th
erearetwowaystousethiscommand.Thefirstisbyspecifyinganintervalofrulen
umberstodothechangeson(directlyafter-C).Syntax:start_nr[:end_nr](use-
L--Lntolisttheruleswiththeirrulenumber).Thedetailsarethesameasforthe-
Dcommand.Thesecondusageisbyspecifyingthecompleteruleasitwouldhavebeen
specifiedwhenitwasadded.Onlythecountersofthefirstencounteredrulethati
sthesameasthisspecifiedrule,inotherwordsthematchingrulewiththelowest(
positive)rulenumber,arechanged.Inthefirstusage,thecountersarespecifie
ddirectlyaftertheintervalspecification,inthesecondusagedirectlyafter-
C.Firstthepacketcounterisspecified,thenthebytecounter.Ifthespecifiedc
ountersstartwitha'+',thecountervaluesareaddedtotherespectivecurrentco
untervalues.Ifthespecifiedcountersstartwitha'-',thecountervaluesarede
creasedfromtherespectivecurrentcountervalues.Noboundscheckingisdone.I
fthecountersdon'tstartwith'+'or'-',thecurrentcountersarechangedtothes
pecifiedcounters.

-I,--insert

Insertthespecifiedruleintotheselectedchainatthespecifiedrulenumbe
r.Iftherulenumberisnotspecified,theruleisaddedattheheadofthechain.Ift
hecurrentnumberofrulesequalsN,thenthespecifiednumbercanbebetween-Nand
N+1.Forapositivenumberi,itholdsthatiandi-N-1specifythesameplaceinthec
hainwheretheruleshouldbeinserted.TherulenumberOspecifiestheplacepastt
helastruleinthechainandusingthisnumberisthereforeequivalenttousingthe
-Acommand.RulenumbersstructlysmallerthanOcanbeusefulwhenmorethanoneru
leneedstobeinsertedinachain.

-P, --policy

Setthepolicyforthechaintothegiventarget. ThepolicycanbeACCEPT, DROP orRETURN.

-F, --flush

Flushtheselectedchain. Ifnochainisselected, theneverychainwillbeflu shed. Flushingachaindoesnotchangethepolicyofthechain, however.

-Z, --zero

Setthecountersoftheselectedchaintozero. Ifnochainisselected, allthe countersaresettozero. The-Zcommandcanbeusedinconjunctionwiththe-Lcomma nd. Whenboththe-Zand-Lcommandsareusedtogetherinthisway, therulecounters areprintedonthescreenbeforetheyaresettozero.

-L, --list

Listallrulesintheselectedchain. Ifnochainisselected, allchainsareli sted.

Thefollowingoptionschangetheoutputofthe-Lcommand.

--Ln

Placestherulenumberinfrontofeveryrule. Thisoptionisincompatiblewit hthe--Lxoption.

--Lc

Showsthecountersattheendofeachruledisplayedbythe-Lcommand. Bothafr amecounter(pcnt)andabytecounter(bcnt)aredisplayed. Theframecountershow showmanyframeshavematchedthespecificrule, thebytecountershowsthesumoft

heframesizesofthesematchingframes.Usingthisoptionincombinationwiththe
--Lxoptioncausesthecounterstobewrittenoutinthe'-c<pcnt><bcnt>'optionf
ormat.

--Lx

Changestheoutputsothatitproducesasetofebtablescommandsthatconstru
ctthecontentsofthechain,whenspecified.Ifnochainisspecified,ebtablesco
mmandstoconstructthecontentsofthetablearegiven,includingcommandsforcr
eatingtheuser-definedchains(ifany).Youcanusethissetofcommandsinanebta
blesbootorreloadscript.Forexampletheoutputcouldbeusedatsystemstartup.
The--Lxoptionisincompatiblewiththe--Lnlistingoption.Usingthe--Lxoptio
ntogetherwiththe--Lcoptionwillcausethecounterstobewrittenoutinthe'-c<
pcnt><bcnt>'optionformat.

--Lmac2

ShowsallMACaddresseswiththesamelength,addingleadingzeroesifnecess
ary.Thedefaultrepresentationomitsleadingzeroesintheaddresses.

-N,--new-chain

Createanewuser-definedchainwiththegivenname.Thenumberofuser-defin
edchainsislimitedonlybythenumberofpossiblechainnames.Auser-definedcha
innamehasamaximumlengthof31characters.Thestandardpolicyoftheuser-defi
nedchainisACCEPT.Thepolicyofthenewchaincanbeinitializedtoadifferentst
andardtargetbyusingthe-Pcommandtogetherwiththe-Ncommand.Inthiscase,th
echainnamedoesnothavetobespecifiedforthe-Pcommand.

-X,--delete-chain

Deletethespecifieduser-definedchain.Theremustbenoremainingreferen
ces(jumps)tothespecifiedchain,otherwiseebtableswillrefusetodeleteit.I

fnochainisspecied, alluser-definedchainsthataren'treferencedwillbere
moved.

-E,--rename-chain

Renamethespecifiedchaintoanewname.Besidesrenamingauser-definedcha
in,youcanrenameastandardchaintoanamethatsuitsyourtaste.Forexample,ify
oulikePREFORWARDINGmorethanPREROUTING,thenyoucanusethe-Ecommandtorena
methePREROUTINGchain.Ifyoudorenameoneofthestandardebtableschainnames,
pleasebesuretomentionthisfactshouldyoupostaquestionontheebtablesmaili
nglists.Itwouldbewisetousethestandardnameinyourpost.Renamingastandard
ebtableschaininthisfashionhasnoeffectonthestructureorfunctioningofthe
ebtableskerneltable.

--init-table

Replacethecurrenttabledatabytheinitialtabledata.

--atomic-init

Copythekernel'sinitialdataofthetabletothespecifiedfile.Thiscanbeu
sedasthefirstaction,afterwhichrulesareaddedtothefile.Thefilecanbespec
ifiedusingthe--atomic-filecommandorthroughtheEBTABLES_ATOMIC_FILEenvi
ronmentvariable.

--atomic-save

Copythekernel'scurrentdataofthetabletothespecifiedfile.Thiscanbeu
sedasthefirstaction,afterwhichrulesareaddedtothefile.Thefilecanbespec
ifiedusingthe--atomic-filecommandorthroughtheEBTABLES_ATOMIC_FILEenvi
ronmentvariable.

--atomic-commit

Replacethekerneltabledatawiththedatacontainedinthespecifiedfile. T
hisisausefulcommandthatallowsyoutoloadallyourrulesofacertaintableinto
thekernelatonce, savingthekernelalotofprecioustimeandallowingatomicupd
atesofthetables. Thefilewhichcontainsthetabledataisconstructedbyusinge
itherthe--atomic-initorthe--atomic-savecommandtogenerateastartingfile
. Afterthat, usingthe--atomic-filecommandwhenconstructingrulesorsetting
theEBTABLES_ATOMIC_FILEenvironmentvariableallowsyoutoextendthefileand
buildthecompletetablebeforecommittingittothekernel. Thiscommandcanbeve
ryusefulinbootscriptstopopulatetheebtablestablesinafastway.

MISCELLANOUSCOMMANDS

-V, --version

Showtheversionoftheebtablesuserspaceprogram.

-h, --help[listofmodulenames]

Giveabriefdescriptionofthecommandsyntax. Hereyoucanalsospecifyname
sofextensionsandebtableswilltrytowritehelpaboutthoseextensions. E. g. eb
tables-hsnatlogiparp. Specifylist_extensionstolistallextensionssupport
edbytheuserspaceutility.

-j, --jumptarget

Thetargetoftherule. Thisisoneofthefollowingvalues:ACCEPT, DROP, CONT
INUE, RETURN, atargetextension(seeTARGETEXTENSIONS)orauser-definedchain
name.

--atomic-filefile

Letthecommandoperateonthespecifiedfile. Thedataofthetabletooperate
onwillbeextractedfromthefileandtheresultoftheoperationwillbesavedback

intothefile. Ifspecified, thisoptionshouldcomebeforethecommandspecifica
tion. Analternativethatshouldbepreferred, issettingtheEBTABLES_ATOMIC_F
ILEenvironmentvariable.

-M, --modprobeprogram

Whentalkingtothekernel, usethisprogramtotrytoautomaticallyloadmiss
ingkernelmodules.

--concurrent

Useafilelocktosupportconcurrentscriptsupdatingtheebtableskernelta
bles.

RULE SPECIFICATIONS

Thefollowingcommandlineargumentsmakeuparulespecification(asusedin
theaddanddeletecommands). A"!"optionbeforethespecificationinvertsthete
stforthatspecification. Apartfromthesestandardrulespecificationstherea
resomeothercommandlineargumentsofinterest. SeeboththeMATCHEXTENSIONSan
dtheWATCHEREXTENSIONSbelow.

-p, --protocol[!]protocol

Theprotocolthatwasresponsibleforcreatingtheframe. Thiscanbeahexade
cimalnumber, above0x0600, aname(e.g. ARP)orLENGTH. TheprotocolfieldoftheE
thernetframecanbeusedtodenotethelengthoftheheader(802.2/802.3networks
). Whenthevalueofthatfieldisbeloworequals0x0600, thevalueequalsthesizeo
ftheheaderandshouldn'tbeusedasaprotocolnumber. Instead, allframeswheret
heprotocolfieldisusedasthelengthfieldareassumedtobeofthesame'protocol
'. TheprotocolnameusedinebtablesfortheseframesisLENGTH.

Thefile/etc/ethertypescanbeusedtoshowreadablecharactersinsteadofh
exadecimalnumbersfortheprotocols.Forexample,0x0800willberepresentedby
IPV4.Theuseofthisfileisnotcasesensitive.Seethatfileformoreinformation
.Theflag--protoisanaliasforthisoption.

-i,--in-interface[!]name

Theinterface(bridgeport)viawhichaframeisreceived(thisoptionisusef
ulintheINPUT,FORWARD,PREROUTINGandBROUTINGchains).Iftheinterfacenamee
ndswith'+',thenanyinterfacenamethatbeginswiththisname(disregarding'+'
)willmatch.Theflag--in-ifisanaliasforthisoption.

--logical-in[!]name

The(logical)bridgeinterfaceviawhichaframeisreceived(thisoptionisu
sefulintheINPUT,FORWARD,PREROUTINGandBROUTINGchains).Iftheinterfacena
meendswith'+',thenanyinterfacenamethatbeginswiththisname(disregarding
'+')willmatch.

-o,--out-interface[!]name

Theinterface(bridgeport)viawhichaframeisgoingtobesent(thisoptioni
susefulintheOUTPUT,FORWARDandPOSTROUTINGchains).Iftheinterfacenameend
swith'+',thenanyinterfacenamethatbeginswiththisname(disregarding'+')w
illmatch.Theflag--out-ifisanaliasforthisoption.

--logical-out[!]name

The(logical)bridgeinterfaceviawhichaframeisgoingtobesent(thisopti
onisusefulintheOUTPUT,FORWARDandPOSTROUTINGchains).Iftheinterfacename
endswith'+',thenanyinterfacenamethatbeginswiththisname(disregarding'+
')willmatch.

-s, --source[!]address[/mask]

The source MAC address. Both mask and address are written as 6 hexadecimal numbers separated by colons. Alternatively one can specify Unicast, Multicast, Broadcast or BGA (Bridge Group Address):

Unicast=00:00:00:00:00:00/01:00:00:00:00:00, Multicast=01:00:00:00:00:00/01:00:00:00:00:00, Broadcast=ff:ff:ff:ff:ff:ff/ff:ff:ff:ff:ff:f for BGA=01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff. Note that a broadcast address will also match the multicast specification. The flag --src is an alias for this option.

-d, --destination[!]address[/mask]

The destination MAC address. See -s (above) for more details on MAC addresses. The flag --dst is an alias for this option.

-c, --set-counter pcnt bcnt

If used with -A or -I, then the packet and byte counters of the new rule will be set to pcnt, resp. bcnt. If used with the -C or -D commands, only rules with a packet and byte count equal to pcnt, resp. bcnt will match.

MATCH EXTENSIONS

Ebtables extensions are dynamically loaded into the userspace tool, there is therefore no need to explicitly load them with a -m option like is done in iptables. These extensions deal with functionality supported by kernel modules supplemental to the core ebtables code.

802_3

Specify 802.3 DSAP/SSAP fields or SNAP type. The protocol must be specified as LENGTH (see the option -p above).

--802_3-sap[!]sap

DSAPandSSAParetwooonebyte802.3fields.Thebytesarealwaysequal,soonly onebyte(hexadecimal)isneededasanargument.

--802_3-type[!]type

Ifthe802.3DSAPandSSAPvaluesare0xaathentheSNAPtypefieldmustbeconsu ltedtodeterminethepayloadprotocol.Thisisatwobyte(hexadecimal)argument .Only802.3frameswithDSAP/SSAP0xaaarecheckedfortype.

among

MatchaMACaddressorMAC/IPaddresspairversusalistofMACaddressesandMA C/IPaddresspairs.Alistentryhasthefollowingformat:xx:xx:xx:xx:xx:xx[=i p.ip.ip.ip][,].Multiplelistentriesareseparatedbyacomma,specifyinganIP addresscorrespondingtotheMACaddressisoptional.MultipleMAC/IPaddresspa irswiththesameMACaddressbutdifferentIPaddress(andviceversa)canbespeci fied.IftheMACaddressdoesn'tmatchanyentryfromthelist,theframedoesn'tma tchtherule(unless"!"wasused).

--among-dst[!]list

ComparetheMACdestinationtothegivenlist.IftheEthernetframehastypeI Pv4orARP,thencomparisonwithMAC/IPdestinationaddresspairsfromthelistis possible.

--among-src[!]list

ComparetheMACsourcetothegivenlist.IftheEthernetframehastypeIPv4or ARP,thencomparisonwithMAC/IPsourceaddresspairsfromthelistispossible.

--among-dst-file[!]file

Sameas--among-dstbutthelistisreadinfromthespecifiedfile.

--among-src-file[!]file

Sameas--among-srcbutthelistisreadinfromthespecifiedfile.

arp

Specify(R)ARPfields.TheprotocolmustbespecifiedasARPorRARP.

--arp-opcode[!]opcode

The(R)ARPopcode(decimalorastring,formoredetailsseeebtables-harp).

--arp-htype[!]hardwaretype

Thehardwaretype,thiscanbeadecimalorthestringEthernet(whichsetstyp
eto1).Most(R)ARPpacketshaveEternetashardwaretype.

--arp-ptype[!]protocoltype

Theprotocoltypeforwhichthe(r)arpisused(hexadecimalorthestringIPv4
,denoting0x0800).Most(R)ARPpacketshaveprotocoltypeIPv4.

--arp-ip-src[!]address[/mask]

The(R)ARPIPsourceaddressspecification.

--arp-ip-dst[!]address[/mask]

The(R)ARPIPdestinationaddressspecification.

--arp-mac-src[!]address[/mask]

The(R)ARPMACsourceaddressspecification.

--arp-mac-dst[!]address[/mask]

The(R)ARPMACdestinationaddressspecification.

[!]--arp-gratuitous

ChecksforARPgratuitouspackets:checksequalityofIPv4sourceaddressan
dIPv4destinationaddressinsidetheARPheader.

ip

SpecifyIPv4fields.TheprotocolmustbespecifiedasIPv4.

--ip-source[!]address[/mask]

ThesourceIPaddress.Theflag--ip-srcisanaliasforthisoption.

--ip-destination[!]address[/mask]

ThedestinationIPaddress.Theflag--ip-dstisanaliasforthisoption.

--ip-tos[!]tos

TheIPtypeofservice,inhexadecimalnumbers.IPv4.

--ip-protocol[!]protocol

TheIPprotocol.Theflag--ip-protoisanaliasforthisoption.

--ip-source-port[!]port1[:port2]

ThesourceportorportrangefortheIPprotocols6(TCP),17(UDP),33(DCCP)o
r132(SCTP).The--ip-protocoloptionmustbespecifiedasTCP,UDP,DCCPorSCTP.
Ifport1isomitted,0:port2isused;ifport2isomittedbutacolonisspecified,p
ort1:65535isused.Theflag--ip-sportisanaliasforthisoption.

--ip-destination-port[!]port1[:port2]

The destination port or port range for ip protocols 6 (TCP), 17 (UDP), 33 (DCCP) or 132 (SCTP). The --ip-protocol option must be specified as TCP, UDP, DCCP or SCTP. If port1 is omitted, 0:port2 is used; if port2 is omitted but a colon is specified, port1:65535 is used. The flag --ip-dport is an alias for this option.

ip6

Specify IPv6 fields. The protocol must be specified as IPv6.

--ip6-source[!]address[/mask]

The source IPv6 address. The flag --ip6-src is an alias for this option.

--ip6-destination[!]address[/mask]

The destination IPv6 address. The flag --ip6-dst is an alias for this option.

--ip6-tclass[!]tclass

The IPv6 traffic class, in hexadecimal numbers.

--ip6-protocol[!]protocol

The IP protocol. The flag --ip6-proto is an alias for this option.

--ip6-source-port[!]port1[:port2]

The source port or port range for the IPv6 protocols 6 (TCP), 17 (UDP), 33 (DCCP) or 132 (SCTP). The --ip6-protocol option must be specified as TCP, UDP, DCCP or SCTP. If port1 is omitted, 0:port2 is used; if port2 is omitted but a colon is specified, port1:65535 is used. The flag --ip6-sport is an alias for this option.

--ip6-destination-port[!]port1[:port2]

ThedestinationportorportrangeforIPv6protocols6(TCP),17(UDP),33(DCCP)or132(SCTP).The--ip6-protocoloptionmustbespecifiedasTCP,UDP,DCCPorSCTP.Ifport1isomitted,0:port2isused;ifport2isomittedbutacolonisspecified,port1:65535isused.Theflag--ip6-dportisanaliasforthisoption.

--ip6-icmp-type[!]{type[:type]/code[:code]|typename}

Specifyipv6-icmptypeandcodetomatch.Rangesforbothtypeandcodearesupported.Typeandcodeareseparatedbyaslash.Validnumbersfortypeandrangeare0to255.Tomatchasingletypeincludingallvalidcodes,symbolicnamescanbeusedinsteadofnumbers.Thelistofknowntypenamesisshownbythecommand

ebtables--helpip6

Thisoptionisonlyvalidfor--ip6-prococolipv6-icmp.

limit

Thismodulematchesatalimitedrateusingatokenbucketfilter.Aruleusingthisextensionwillmatchuntilthislimitisreached.Itcanbeusedwiththe--logwatchertogivelimitedlogging,forexample.Itsuseisthesameasthelimitmatchofiptables.

--limit[value]

Maximumaveragematchingrate:specifiedasanumber,withanoptional/second,/minute,/hour,or/daysuffix;thedefaultis3/hour.

--limit-burst[number]

Maximuminitialnumberofpacketstomatch:thisnumbergetsrechargedbyoneeverytimethelimitspecifiedaboveisnotreached,uptothisnumber;thedefaultis5.

mark_m

--mark[!][value][/mask]

Matches frames with the given unsigned mark value. If a value and mask are specified, the logical AND of the mark value of the frame and the user-specified mask is taken before comparing it with the user-specified mark value. When only a mark value is specified, the packet only matches when the mark value of the frame equals the user-specified mark value. If only a mask is specified, the logical AND of the mark value of the frame and the user-specified mask is taken and the frame matches when the result of this logical AND is non-zero. Only specifying a mask is useful to match multiple mark values.

pkttype

--pkttype-type[!]type

Matches on the Ethernet "class" of the frame, which is determined by the generic networking code. Possible values: broadcast (MAC destination is the broadcast address), multicast (MAC destination is a multicast address), host (MAC destination is the receiving network device), or otherhost (none of the above).

stp

Specify stp BPDU (bridge protocol data unit) fields. The destination address (-d) must be specified as the bridge group address (BGA). For all options for which a range of values can be specified, it holds that if the lower bound is omitted (but the colon is not), then the lowest possible lower bound for that option is used, while if the upper bound is omitted (but the colon again is not), the highest possible upper bound for that option is used.

--stp-type[!]type

TheBPDUtype(0-255),recognizednon-numericaltypesareconfig,denoting aconfigurationBPDU(=0),andtcn,denothingatopologychangenotificationBPD U(=128).

--stp-flags[!]flag

TheBPDUflag(0-255),recognizednon-numericalflagsaretopology-change ,denotingthetopologychangeflag(=1),andtopology-change-ack,denotingthe topologychangeacknowledgementflag(=128).

--stp-root-prio[!][prio][:prio]

Therootpriority(0-65535)range.

--stp-root-addr[!][address][/mask]

Therootmacaddress,seetheoption-sformoredetails.

--stp-root-cost[!][cost][:cost]

Therootpathcost(0-4294967295)range.

--stp-sender-prio[!][prio][:prio]

TheBPDU'ssenderpriority(0-65535)range.

--stp-sender-addr[!][address][/mask]

TheBPDU'ssendermacaddress,seetheoption-sformoredetails.

--stp-port[!][port][:port]

Theportidentifier(0-65535)range.

--stp-msg-age[!][age][:age]

The message age timer (0-65535) range.

--stp-max-age[!][age][:age]

The max age timer (0-65535) range.

--stp-hello-time[!][time][:time]

The hello time timer (0-65535) range.

--stp-forward-delay[!][delay][:delay]

The forward delay timer (0-65535) range.

vlan

Specify 802.1Q Tag Control Information fields. The protocol must be specified as 802_1Q (0x8100).

--vlan-id[!]id

The VLAN identifier field (VID). Decimal number from 0 to 4095.

--vlan-prio[!]prio

The user priority field, a decimal number from 0 to 7. The VID should be set to 0 ("null VID") or unspecified (in the latter case the VID is deliberately set to 0).

--vlan-encap[!]type

The encapsulated Ethernet frame type/length. Specified as a hexadecimal number from 0x0000 to 0xFFFF or as a symbolic name from /etc/ethertypes.

WATCHER EXTENSIONS

Watchersonlylookatframespassingby, theydon'tmodifythemnordecidetoa ccepttheframesornot. Thesewatchersonlyseetheframeiftheframematchesther ule, andtheyseeitbeforethetargetisexecuted.

log

Thelogwatcherwritesdescriptivedataaboutaframetothesyslog.

--log

Logwiththedefaultlogginoptions:log-level=info, log-prefix="", noipl ogging, noarplogging.

--log-levellevel

Definesthelogginglevel. Forthepossiblevalues, seeebtables-hlog. Thed efaultlevelisinfo.

--log-prefixtext

Definestheprefixtexttobeprintedatthebeginningofthelinewiththelogg inginformation.

--log-ip

Willlogtheipinformationwhenaframemadebytheipprotocolmatchestherul e. Thedefaultisnoipinformationlogging.

--log-ip6

Willlogtheipv6informationwhenaframemadebytheipv6protocolmatchesth erule. Thedefaultisnoipv6informationlogging.

--log-arp

Willlogthe(r)arpinformationwhenaframemadebythe(r)arpprotocolsmatc
hestherule.Thedefaultisno(r)arpinformationlogging.

nflog

Thenflogwatcherpassesthepackettotheloadedloggingbackendinordertol
ogthepacket.Thisisusuallyusedincombinationwithnfnetlink_logasloggingb
ackend,whichwillmulticastthepacketthroughanetlinksockettothespecified
multicastgroup.Oneormoreuserspaceprocessesmaysubscribetothegrouptorec
eivethepackets.

--nflog

Logwiththedefaultloggingoptions

--nflog-groupnlgroup

Thenetlinkgroup($1-2^{32}-1$)towhichpacketsare(onlyapplicablefornfnet
link_log).Thedefaultvalueis1.

--nflog-prefixprefix

Aprefixstringtoincludeinthelogmessage,upto30characterslong,useful
fordistinguishingmessagesinthelogs.

--nflog-rangesize

Thenumberofbytestobecopiedtouserspace(onlyapplicablefornfnetlink_
log).nfnetlink_loginstancesmayspecifytheirownrange,thisoptionoverride
sit.

--nflog-thresholdsize

Numberofpacketstoqueueinsidethekernelbeforesendingthemtouserspace(onlyapplicablefornfnetlink_log).Highervaluesresultinlessoverheadperpacket,butincreasedelayuntilthepacketsreachuserspace.Thedefaultvalueis1.

ulog

Theulogwatcherpassesthepackettouserspaceloggingdaemonusingnetlinkmulticastsockets.Thisdiffersfromthelogwatcherinthesensethatthecompletepacketissenttouserspaceinsteadofadescriptivetextandthatnetlinkmulticastsocketsareusedinsteadofthesyslog.Thiswatcherenablesparsingofpacketswithuserspaceprograms,thephysicalbridgeinandoutportsarealsoincludedinthenetlinkmessages.Theulogwatchermoduleaccepts2parameterswhenthemoduleisloadedintothekernel(e.g.withmodprobe):nlbufsizspecifieshowbigthebufferforeachnetlinkmulticastgroupis.Ifyousaynlbufsiz=8192,forexample,uptoeightkBofpacketswillgetaccumulatedinthekerneluntiltheyaresenttouserspace.Itisnotpossibletoallocatemorethan128kB.Pleasealsokeepinmindthatthisbuffersizeisallocatedforeachnlgroupyouareusing,sothetotalkernelmemoryusageincreasesbythatfactor.Thedefaultis4096.flushtimeoutspecifiesafterhowmanyhundredthsofasecondthequeueshouldbeflushed,evenifitisnotfullyet.Thedefaultis10(onetenthofasecond).

--ulog

Usethedefaultsettings:ulog-prefix="",ulog-nlgroup=1,ulog-cprange=4096,ulog-qthreshold=1.

--ulog-prefixtext

Definestheprefixincludedwiththepacketssenttouserspace.

--ulog-nlgroupgroup

Defineswhichnetlinkgroupnumbertouse(anumberfrom1to32).Makesurethe netlinkgroupnumbersusedfortheiptablesULOGtargetdifferfromthoseusedfor theebtablesulogwatcher.Thedefaultgroupnumberis1.

--ulog-cprangerange

Definesthemaximumcopyrangetouserspace,forpacketsmatchingtherule.T hedefaultrangeis0,whichmeansthemaximumcopyrangeisgivenbynlbufsiz.Amax imumcopyrangelargerthan128*1024ismeaninglessasthepacketssenttouserspa cehaveanuppersizelimitof128*1024.

--ulog-qthresholdthreshold

Queueatmostthresholdnumberofpacketsbeforesendingthemtouserspacewi thanetlinksocket.Notethatpacketscanbesenttouserspacebeforethequeueisf ull,thishappenswhentheulogkerneltimergoesoff(thefrequencyofthistimerd ependsonflushtimeout).

TARGET EXTENSIONS

arpreply

ThearpreplytargetcanbeusedinthePREROUTINGchainofthenattable.Ifthi stargetseesanARPrequestitwillautomaticallyreplywithanARPreply.Theused MACaddressforthereplycanbespecified.TheprotocolmustbespecifiedasARP.W hentheARPmessageisnotanARPrequestorwhentheARPrequestisn'tforanIPaddre ssonanEthernetnetwork,itisignoredbythistarget(CONTINUE).WhentheARPreq uestismalformed,itisdropped(DROP).

--arpreply-macaddress

SpecifiestheMACaddresstoreplywith:theEthernetsourceMACandtheARPpa yloadsourceMACwillbefilledinwiththisaddress.

--arpreply-targettarget

Specifiesthestandardtarget.AftersendingtheARPreply,therulestillha
stogiveastandardtargetsoebtablesknowswhattodowiththeARPrequest.Thedef
aulttargetisDROP.

dnat

ThednattargetcanonlybeusedintheBROUTINGchainofthebroutetableandth
ePREROUTINGandOUTPUTchainsofthenattable.Itspecifiesthatthedestination
MACaddresshastobechanged.

--to-destinationaddress

ChangethedestinationMACaddresstothespecifiedaddress.Theflag--to-d
stisanaliasforthisoption.

--dnat-targettarget

Specifiesthestandardtarget.Afterdoingthednat,therulestillhastogiv
eastandardtargetsoebtablesknowswhattodowiththednatedframe.Thedefaultt
argetisACCEPT.MakingitCONTINUEcouldletyouusemultipletargetextensionso
nthesameframe.MakingitDROPonlymakessenseintheBROUTINGchainbutusingthe
redirecttargetismorelogicalthere.RETURNisalsoallowed.NotethatusingRET
URNinabasechainisnotallowed(forobviousreasons).

mark

Themarktargetcanbeusedineverychainofeverytable.Itispossibletouset
hemarkingofaframe/packetinbothebtablesandiptables,ifthebridge-nfcodei
scompiledintothekernel.Bothputthemarkingatthesameplace.Thisallowsfora
formofcommunicationbetweenebtablesandiptables.

--mark-setvalue

Mark the frame with the specified non-negative value.

--mark-or value

Or the frame with the specified non-negative value.

--mark-and value

And the frame with the specified non-negative value.

--mark-xor value

Xor the frame with the specified non-negative value.

--mark-target target

Specifies the standard target. After marking the frame, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE can let you do other things with the frame in subsequent rules of the chain.

redirect

The redirect target will change the MAC target address to that of the bridge device the frame arrived on. This target can only be used in the BROUTING chain of the broute table and the PREROUTING chain of the nat table. In the BROUTING chain, the MAC address of the bridge port is used as destination address, in the PREROUTING chain, the MAC address of the bridge is used.

--redirect-target target

Specifies the standard target. After doing the MAC redirect, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE could let you use multiple target extensions on the same fra

me. MakingitDROPintheBROUTINGchainwilllettheframesberouted. RETURNisals oallowed. NotethatusingRETURNinabasechainisnotallowed.

snat

ThesnattargetcanonlybeusedinthePOSTROUTINGchainofthenattable. Itsp ecifiesthatthesourceMACaddresshastobechanged.

--to-sourceaddress

ChangesthesourceMACaddresstothespecifiedaddress. Theflag--to-srcis analiasforthisoption.

--snat-targettarget

Specifiesthestandardtarget. Afterdoingthesnat, therulestillhastogiv eastandardtargetsoebtablesknowswhattodo. ThedefaulttargetisACCEPT. Maki ngitCONTINUEcouldletyouusemultipletargetextensionsonthesameframe. Maki ngitDROPdoesn'tmakesense, butyoucoulddothattoo. RETURNisalsoallowed. Not ethatusingRETURNinabasechainisnotallowed.

--snat-arp

Alsochangethehardwaresourceaddressinsidethearpheaderifthepacketis anarpmessageandthehardwareaddresslengthinthearpheaderis6bytes.