

Frequently Asked Questions

Question

Netflow = 0 FreeBSD ?> 4 A G 5 B B @ 0 D 8 : 0

Answer

Netflow - > 48 = 87 A 0 < KE C 4 > 1 = KE A ? > A > 1 > 2 A 1 > @ 0 B @ 0 D 8 : 0 4 ; O
 = 8 : A A 8 A B 5 < . ! C G 5 B > < B > 3 > G B > > = A > 2 < 5 A B 8 < A D ; > C
 ? @ > B > : > ; > < Cisco 8 A ? > A > 15 = A > 18 @ 0 B L \ > B 4 0 2 0 B L 4 0 == K 5
 ? > A 5 B 8, A 8 A B 5 < 0 ? @ 5 4 A B 0 2 ; O 5 B A > 1 > 9 > A > 1 K 9 8 = B 5 @ 5 A. > B
 = 5 ? ; > E 0 O A A K ; : 0 A > ? 8 A 0 = 8 5 < = 5 B 3 @ 0 D: [' > www.opennet.ru](http://www.opennet.ru)

A ; 8 2 4 2 C E A ; > 2 0 E, B > 8 4 5 > ; > 3 8 O netgraph ? > 7 2 > ; O 5 B ? C B 5 <
 A > 7 4 0 = 8 O 2 8 7 C 0 ; L = KE 3 @ 0 D > 2 8 7 " : C 1 8 : > 2 " ? @ > B > : > ; > 2,
 ? > @ B > 2 8 A 5 @ 2 8 A > 2 : 0 : 1 K A B @ > 8 B L 2 7 0 8 < > 4 5 9 A B 2 8 5 A 5 B 5 2 K E
 : > < ? > = 5 = B > 2 ? @ > A B K < A > 7 4 0 = 8 5 < A 2 O 7 5 9 < 5 6 4 C
 " : C 1 8 : 0 < 8".
 ' B > = C 6 = > G B > 1 K C A B 0 = > 2 8 B L M B > 2 A 5 = 0 FreeBSD ? ; O = 0 G 0 ; 0
 = 0 1 > @ 2 : ; N G 5 = 8 9 2 O 4 @ > 4 ; O > 1 5 A ? @ 5 G 5 = 8 O ? > 4 4 5 @ 6 : 8
 netgraph. > ; = 0 O 2 5 @ A 8 O (> = 0 = 0 A 0 < > < 4 5 ; 5 = 5 = C 6 = 0 2 B 0 : > <
 : > ; 8 G 5 A B 2 5, 4 ; O ? > 4 A G 5 B 0 B @ 0 D 8 : 0 4 > A B 0 B > G = > < 5 = L H 5 3 >):

<i>options</i>	<i>NETGRAPH</i>	<i>#netgraph(4) system</i>
<i>options</i>	<i>NETGRAPH_ASYNC</i>	
<i>options</i>	<i>NETGRAPH_BPF</i>	
<i>options</i>	<i>NETGRAPH_CISCO</i>	
<i>options</i>	<i>NETGRAPH_ECHO</i>	
<i>options</i>	<i>NETGRAPH_ETHER</i>	
<i>options</i>	<i>NETGRAPH_FRAME_RELAY</i>	
<i>options</i>	<i>NETGRAPH_HOLE</i>	
<i>options</i>	<i>NETGRAPH_IFACE</i>	
<i>options</i>	<i>NETGRAPH_KSOCKET</i>	
<i>options</i>	<i>NETGRAPH_L2TP</i>	
<i>options</i>	<i>NETGRAPH_LMI</i>	
# MPPC compression requires proprietary files (not included)		
<i>#options</i>	<i>NETGRAPH_MPPC_COMPRESSION</i>	
<i>options</i>	<i>NETGRAPH_MPPC_ENCRYPTION</i>	
<i>options</i>	<i>NETGRAPH_ONE2MANY</i>	
<i>options</i>	<i>NETGRAPH_PPP</i>	
<i>options</i>	<i>NETGRAPH_PPPOE</i>	
<i>options</i>	<i>NETGRAPH_PPTPGRE</i>	
<i>options</i>	<i>NETGRAPH_RFC1490</i>	
<i>options</i>	<i>NETGRAPH_SOCKET</i>	
<i>options</i>	<i>NETGRAPH_TEE</i>	

options **NETGRAPH_TTY**
options **NETGRAPH_UI**
options **NETGRAPH_VJC**

8=8<0;L=> 4>AB0B>G=> 2>B MB>3>:

options **NETGRAPH**
options **NETGRAPH_ETHER**
options **NETGRAPH_SOCKET**
options **NETGRAPH_TEE**

>A;5 B>3> :0: O4 @> 1C45B ?5 @5:><?8;8 @>20=> 8 2A5
70 @01>B05B ?>A;5 ?5 @5703 @C7:8, <>6=> 70=OBLAO
=0AB @>9:>9 :>=: @5B8:8.
>B ? @8<5 @ A >?8A0=85<, 7040G0- A>18 @0BL B @0D8: A
=5:>53> 8=B5 @D59A0 (fxp0) 8 >B ? @02;OBL 53> =0 C40;5==CN
A8AB5<C. -B>B ? @8<5 @ >G5=L E> @>H> >?8AK205B :064>5
459AB285, E>BO 4;O @50;L=>3> A5 @25 @0 =5? @8<5=8<> B. :.
8<55B 8A:;NG8B5;L=> ?>7=020B5;L=K9 284 (:CA:8 A
>?8A0=85< 27OBK A A09B0 nexus.org.ua):

?8H5<":C18:8" netgraph, :>B> @K5 =0< ?>B @51CNBAO:

- :C18: A5B52>3> 8=B5 @D59A0, 2 =0H5< A;CG05fxp0, >=
A>7405BAO 02B><0B8G5A:8. <55B 4;O EC:0: lower 8 upper.
Lower >7=0G05B @01>BC A ? @>B>:>;0<8 =87:>3> C @>2=O, upper -
A>>B25BAB25==> 25 @E=53>. 0A 1C45B 8=B5 @5A>20BL :0:
@07 A5B52>9 ?>B>:,
? @>E>4OI89 >B =86=53> A5B52>3> C @>2=O : 25 @E=5<C.
- :C18: tee. 3> =0< ?>B @51C5BAO A>740BL 2 @CG=CN. <55B
G5BK @5 EC:0: left, right, left2right 8 right2left.
07=0G5=85 MB>3> :C18:0- ? @>?CA:0BL ?0:5BK A left 2 right (8
=0>1> @>B) 8 4C1;8 @>20BL ? @>E>4OI89 ?>B>: 40==KE 2
EC:8
left2right 5A;8 =C6=K 40==K5, :>B> @K5 84CB A;520 =0? @02>
(8AE>4OI89 B @0D8:), 8 right2left 5A;8 40==K5 84CB A ? @020
=0;52>(2E>4OI89 B @0D8:).
- :C18: one2many, =0720=85 3>2> @8B A0<> 70 A51O. @8=8<05B >B
<=>38E EC:>2 (many0,many1,many2 8 B. 4.) 8 ?5 @5405B "A>18 @0O" ?>B>: 8
2 >48= EC:one.
- :C18: netflow, :>B> @K9 1C45B ? @8=8<0BL =0 A51O A5B52K5
?>B>:8 A=OBK5 ? @8 ?><>I8tee C A5B52KE 8=B5 @D59A>2

G 5 @ 5 7 E C : 8 iface0, iface1, iface2 8 B. 4.

- B > B : C 1 8 : 1 C 4 5 B D > @ < 8 @ > 2 0 B L cisco netflow ? 0 : 5 B K, A > 4 5 @ 6 0 1 8 5

0 3 @ 5 3 3 8 @ > 2 0 == C N 8 = D > @ < 0 F 8 N > ? @ > H 5 4 H 5 < B @ 0 D 8 : 5 8

? 5 @ 5 4 0 2 0 B L 2 E C : export.

5. : C 1 8 : ksocket, A B 0 = 4 0 @ B = K 9 < > 4 C ; L netgraph 4 ; O > B ? @ 0 2 : 8 ? 0 : 5 B > 2

> ? @ 5 4 5 ; 5 == > < C E > A B C. = 0 H 5 < A ; C G 0 5 = 0 E C : inet/dgram/udp

1 C 4 C B ? > A B C ? 0 B L > B netflow ? 0 : 5 B K 4 ; O ? 5 @ 5 4 0 G 8 E > A B C.

? @ 0 2 ; O N 1 8 < A > > 1 1 5 = 8 5 < msg < K 7 0 4 0 4 8 < E > A B 8 ? > @ B, = 0

: > B > @ K 9 1 C 4 C B C E > 4 8 B L = 0 H 8 ? 0 : 5 B K (192.168.1.10:2055).

! > 7 4 0 B L C 7 5 ; < > 6 == ? @ 8 ? > < > 1 8 : > < 0 = 4 K mkpeer, ? @ 8 G 5 <

A > 7 4 0 = 8 5 C 7 ; 0 2 A 5 3 4 0 ? @ > 8 A E > 4 8 B A ? > 4 : ; N G 5 = 8 5 <

> 4 == > 3 > 8 7 E C : > 2 A > 7 4 0 2 0 5 < > 3 > C 7 ; 0

: E C : C @ > 4 8 B 5 ; L A : > 3 > C 7 ; 0, 8 ? @ 0 2 4 0, 7 0 G 5 < = 0 <

A > 7 4 0 2 0 B L = 5 ? > 4 : ; N G 5 == K 9 C 7 5 ; ?

! > 5 4 8 = 5 = 8 5 E C : > 2 ? @ > 8 A E > 4 8 B ? @ 8 ? > < > 1 8 : > < 0 = 4 K connect,

A 8 = B 0 : A 8 A : > B > @ > 9 B 0 : > 2:

connect ? 5 @ 2 0 O == > 4 0 2 B > @ 0 O == > 4 0 E C : ? 5 @ 2 > 9 == > 4 K

E C : 2 B > @ > 9 == > 4 K.

< 5 == > 2 0 = 8 5 E C : > 2 8 == > 4 A ; 5 4 C N I 5 5. 0 6 4 K 9 A > 7 4 0 2 0 5 < K 9

== > 4 1 5 7 K < O == K 9, == > 8 < 5 5 B 8 = 4 5 : A, : > B > @ K 9 < K < > 6 5 <

C 2 8 4 5 B L : > < 0 = 4 > 9 list.

@ 8 < 5 @:

Name: ngctl27877 Type: socket ID: 00000009 Num hooks: 0

Name: Type: ksocket ID: 00000008 Num hooks: 1

K < > 6 5 < > 1 @ 0 B 8 B L A O : C 7 ; C ksocket G 5 @ 5 7 5 3 > == > < 5 @ (ID) B 0 : [8]:

2 > 5 B > G 8 5 C : 0 7 K 2 0 5 B = 0 B >, G B > M B > == > 4 0

K < > 6 5 < 4 0 B L

= 0 7 2 0 = 8 5 == > 4 5.

? @ 8 < 5 @ C, = 0 7 > 2 5 < M B > B 6 5 C 7 5 ; : 0 : ksocket1.

name [8]: ksocket1

4 0 ; 5 5 < K C 6 5 < > 6 5 < > 1 @ 0 1 0 B L A O : = 5 < C : 0 : : ksocket1:

> ; 5 7 = 0 : > < 0 = 4 0 show, : > B > @ 0 O = 0 < ? > : 0 6 5 B A > 5 4 8 = 5 == K 5

E C : 8

+ show netflow:

Name: netflow Type: netflow ID: 00000007 Num hooks: 2

Local hook	Peer name	Peer type	Peer ID	Peer hook
export	ksocket	00000008	inet/dgram/udp	
iface0	one2many0	one2many	00000006	one

4 5 A L 2 8 4 = K : 0 : 8 5 E C : 8 5 A B L , A : > ; L : > 8 E , 8 : : 0 : 8 < C 7 ; 0 <
? > 4 : ; N G 5 = K.

= > 4 0 < 8 E C : 0 < < K < > 6 5 < > 1 @ 0 B 8 B L A O @ 0 7 = K < 8
A ? > A > 1 0 < 8 . 0 ? @ 8 < 5 @ , C = 0 A 5 A B L 4 2 0 C 7 ; 0 : tee (E C : 8 left, right, right2left,
left2right) A = 0 7 2 0 = 8 5 < tee1 8 one2many (E C : 8 many0, many1, one) A = 0 7 2 0 = 8 5 < one2many1.
> ? C A B 8 < < K E > B 8 < A > 5 4 8 = 8 B L tee1 G 5 @ 5 7 E C : left : E C : C many0
C 7 ; 0 one2many1, 8 E C : right tee1 : E C : C many1 C 7 ; 0 one2many1.
% C : left > B C 7 ; 0 tee1 0 4 @ 5 A C 5 < : 0 : tee1:left. % C : many0 0 4 @ 5 A C 5 < : 0 :
one2many1:many0.

+ connect tee1: one2many1: left many0

? > A ; 5 B > 3 > : 0 : = > 4 K A > 5 4 8 = 5 = K < K 8 < 5 5 < 2 > 7 < > 6 = > A B L
8 A ? > ; L 7 > 2 0 B L 0 ; L B 5 @ = 0 B 8 2 = C N 0 4 @ 5 A 0 F 8 N , : ? @ 8 < 5 @ C , :
= > 4 5 one2many1 < K < > 6 5 < > 1 @ 0 B 8 B L A O G 5 @ 5 7 = > 4 C tee1
A ; 5 4 C N I 8 < > 1 @ 0 7 > < : tee1:left, 4 0 - 4 0 , : 0 : 1 C 4 - B > < K 0 4 @ 5 A C 5 < E C :
- B C : > = A B @ C : F 8 N < > 6 = > 8 A ? > ; L 7 > 2 0 B L 2
A 2 5 6 5 A > 7 4 0 = = K E , 5 I 5 = 5 8 < 5 = > 2 0 = = K E C 7 ; 0 E.

B 0 ; , = 0 G = 5 < .

> 4 3 @ C 7 8 < 2 O 4 @ > < > 4 C ; L netflow:

:~#kldload ng_netgraph

7 0 ? C A : 0 5 < ngctl

:~#ngctl

8 ? > ? 0 4 0 5 < 2 : > < 0 = 4 = C N A B @ > : C netgraph.
A ; 5 4 C 5 B ? @ > 2 5 @ 8 B L , G B > " : C 1 8 : " netflow 1 K ; : > @ @ 5 : B = >
? > 4 3 @ C 6 5 =:

+ types

There are 20 total types:

Type name	Number of living nodes
netflow	0

```

+ mkpeer fxp0: tee lower left
#### A > 7 4 0 B L C 7 5 ; B 8 ? 0 tee A > 5 4 8 = 0 0 8 E E C : 8
lower 8 left
+ name fxp0:lower tee0
#### = 0 7 2 0 B L A > 7 4 0 = = K 9 C 7 5 ; tee0
+ connect fxp0: fxp0:lower upper right
#### A > 5 4 8 = 0 5 < E C : 8 upper 8 right
+ mkpeer tee0: one2many left2right many0
#### A > 7 4 0 5 < C 7 5 ; B 8 ? 0 one2many A > 5 4 8 = 0 0 E C : 8
left2right 8 many0
+ name tee0:left2right one2many0
#### = 0 7 K 2 0 5 < C 7 5 ; one2many0
+ connect tee0: one2many0: right2left many1
+ mkpeer one2many0: netflow one iface0
#### A > 7 4 0 5 < netflow C 7 5 ;
+ name one2many0:one netflow
+ mkpeer netflow: ksocket export inet/dgram/udp
#### A > 7 4 0 = 8 5 C 7 ; 0 ksocket, A > 5 4 8 = 0 5 < A netgraph
= 0 E C : iten/dgram/udp
+ msg netflow: setifindex { iface=0 index=4 }
#### 7 0 4 0 5 < 8 = 4 5 : A 8 = B 5 @ D 5 9 A 0 ( O B 0 :
? > = 8 < 0 N M B > G B > - B > 2 @ > 4 5 ? > @ 0 4 : > 2 > 3 >
= > < 5 @ 0, ? > 4 : > B > @ K < > = 8 4 5 B 2 ifconfig)
+ msg netflow:export connect inet/192.168.0.12:9996
### 3 > 2 > @ 8 < > B ? @ 0 2 ; O B L ? 0 : 5 B K = 0 E > A B
A 1 > @ 0 A B 0 B 8 A B 8 : 8

```

```

MB>< ? @ 8 < 5 @ 5 @ 0 A A < > B @ 5 = > ? > 4 ; ; NG 5 = 8 5 : A B 0 B 8 A B 8 : 5
> 4 = > 3 > 8 = B 5 @ D 5 9 A 0. > 4 ; ; NG 5 = 8 5 = 5 A : > ; L : 8 E
8 = B 5 @ D 5 9 A > 2 ? @ > 8 A E > 4 8 B 0 = 0 ; > 3 8 G = >, G 5 @ 5 7 tee, one2many 8
> 4 8 = 8 7 A 2 > 1 > 4 = K E E C : > 2 ng_netflow (iface1,iface2, ...) A ; 8 2 A 5 ? @ > H ; >
: 0 : A ; 5 4 C 5 B, B > 192.168.1.10 = 0 G = 5 B ? > ; C G 0 B L netflow ? 0 : 5 B K = 0 UDP
? > @ B 2055.

```

```

@ 8 < 5 @ > G 5 = L E > @ > H > > ? 8 A K 2 0 5 B G B > 4 5 ; 0 5 B A O, : 0 : 8 4 ; O
G 5 3 >. > 4 5 ; > 2 B > < G B > > ? 8 A 0 = = K 9 A ; C G 0 9 A > 7 4 0 5 B
F 8 A : > ? > 4 > 1 = K 9 @ C B 5 @, A ? > A > 1 = K 9 B > ; L : > > B 4 0 2 0 B L
4 0 = = K 5 > B @ 0 D 8 : 5 : C 4 0 - B > = 0 @ C 6 C. B > < C 6 5 O 2 = > = C 6 = >
2 A 5 M B > 4 5 ; > 0 2 B > < 0 B 8 7 8 @ > 2 0 B L 8 2 > A A B 0 = 0 2 ; 8 2 0 B L ? @ 8
: @ 0 H 0 E 8 ; 8 ? 5 @ 5 7 0 ? C A : 5.

```

```
2B><0B8G5A:>5 2>AAB0=>2;5=85 B@0D8:>A1>@0
@50;87C5BAO C <5=O=0 A5@25@5 2>B B0:8< 2>B A:@8?B><:
```

nep63-57# more FlowStart

22

```
=CB@8=8G53>=>2>3>, :0: @07 @50;87>20=0 >B40G0
B@0D8:0=02 E>AB0, A>1AB25==>=0 A51O(127.0.0.1) 8=0=5:89
91.123.123.3 ?> ?> @B0<2055. 0?CA:05BAO MB>B A:@8?B A:><0=4=>9
AB@>:8 8;8 ? @8 703@C7:5=0? @8<5@ 2>B B0::
```

```
FlowStart start vlan998
FlowStart start vlan277
FlowStart start vlan997
```

```
:><?;5:B5 A=0?8A0==K< <=>9 18;;8=3><ProvAdmin(818B5
745AL 65=0 A09B5) 70?CA: ? @>A;CH:8 8=B5@D59A>2
? @>8AE>48B 2 ? @>F5AA5 A>740=8O A?8A:0vlan 4;O :;85=B>2
? @8 70?CA:5 A5@25@0. 0?><=NB>;L:> >48= =N0=A,
A>740==K9 :>=D83 4;O 40==>3>vlan 1C45B A;CH0BL=0=5<
B@0D8: B>;L:> 4> <><5=B0 ?5@5A>740=8O MB>3> 2;0=. "0:
65<>3CB<5=OBLAO 8=45:AK A>740==KE 2;0= 2 A8AB5<5
=5B3@0D. -B> <>65B 2K720BL ? @5:@015=85 ? @>A;CH:8 8
?>B5@N 40==KE. AB5AB25==>, A D878G5A:8<8 8B5@D59A0<8
B0:>5=5 ? @>8AE>48B. 'B>1K 871560BL ?>4>1=KE
? @>1;5<, 5A;8 20<=5>1E>48<> A;CH0BL 8<5==>vlan,
A45;09B5 8E 4> 70?CA:0 :;85=BA:8E 8=B5@D59A>2,
=0? @8<5@ ? @02:>9rc.conf:
```

```
cloned_interfaces="vlan2 vlan997 vlan998"
ifconfig_vlan2="inet 192.168.254.1 netmask 255.255.255.0 vlan 2 vlandev
vr0" #Upravlenie
ifconfig_vlan997="inet 91.123.123.123 netmask 255.255.255.248 vlan 997
vlandev fxp0"
ifconfig_vlan998="inet 84.123.123.123 netmask 255.255.255.252 vlan 998
vlandev fxp0"
```

```
">340;N1K5 87<5=5=8O 2 :;85=BA:8E 2;0= 8=B5@D59A0E
=5 70B @>=CB 8=45:AK 20H8E ? @>A;CH8205<KE 8=B5@D59A>2
8=5 2K7>2CB ?>B5@N 40==KE.
```

" 5 ? 5 @ L G B > : 0 A 0 5 B A O G 0 A B 8 " A 5 @ 2 5 @ ". 0 : 8 G 5 < ? @ 8 = 8 < 0 B L
B > G B > ? @ 8 E > 4 8 B ? > ? > @ B C 2 0 5 5 ? ; O M B > 3 > A C I 5 A B 2 C 5 B = 0 1 > @
flow-tools (/usr/ports/net-mgmt/flow-tools) 8 7 ? > @ B > 2 FreeBSD. @ 8 ? > < > I 8 M B > 3 >
= 0 1 > @ 0 2 K A < > 6 5 B 5 A > 7 4 0 B L : > ; ; 5 : B > @ , ? @ 8 = 8 < 0 N I 8 9
B @ 0 D 8 : > B ; N 1 > 3 > C A B @ > 9 A B 2 0 , = 0 ? @ 0 2 ; O N I 5 3 > = 0 = 5 3 >
? > B > : 2 D > @ < 0 B 5 flow 5 8 ; 8 4 . ! @ 5 4 8 = 8 E > ? 8 A 0 = = K 9 2 K H 5 @ C B 5 @ 8
Cisco = 0 ? @ 8 < 5 @ . # A B 0 = 0 2 ; 8 2 0 5 B 5 B > ; A K 8 7 ? > @ B > 2 , 7 0 B 5 <
A C I 5 A B 2 C 5 B = 5 A : > ; L : > 2 0 @ 8 0 = B > 2 : > ; ; 5 : B > @ 0 . = 5
1 > ; L H 5 = @ 0 2 8 B A O " A : @ 8 ? B > 2 K 9 " 2 0 @ 8 0 = B , > = ? > 7 2 > ; O 5 B
: > = B @ > ; 8 @ > 2 0 B L ? > cron A > A B > O = 8 5 ? @ > A ; C H : 8 ? > @ B > 2 8
C ? @ 0 2 ; O B L ? 0 @ 0 < 5 B @ 0 < 8 . ! > 7 4 0 5 B A O 2 A : @ 8 ? B 0 , 1 - 4 ; O 7 0 ? C A : 0
8 : > = B @ > ; O :

nep63-57# more flow-capture-recovery.sh

22

- B > B ? @ > A B > : 0 6 4 K 9 G 0 A ? @ 5 2 @ 0 I 0 5 B ? @ 8 = O B K 5 4 0 = = K 5 8 7
1 8 = 0 @ = > 3 > 2 8 4 0 2 B 5 : A B > G 8 B 0 5 < K 9 , 3 > B > 2 K 9 : > 1 @ 0 1 > B : 5
2 A O : 8 < 8 @ 0 7 = K < 8 1 8 ; ; 8 = 3 0 < 8 . ! > 1 A B 2 5 = = > , 8 2 A 5 ...

A B L > 4 8 = < 0 ; 5 = L : 8 9 = N 0 = A ... A ; 8 A 5 @ 2 5 @ A ; 8 H : > <
7 0 3 @ C 6 5 = , flow-capture < > 6 5 B = 0 ? @ > G L ? > B 5 @ O B L A 2 O 7 L A
" @ 5 0 ; L = > A B L N " 8 ? 5 @ 5 A B 0 B L A > 1 8 @ 0 B L B @ 0 D 8 : . 1 M B > <
C ? > < 8 = 0 5 B A O 2 5 3 > < 0 = 0 E . 0 M B > B A ; C G 0 9 < > 6 5 B ? > < > G L
4 @ C 3 > 9 ? > 4 E > 4 , : > B > @ K 9 > ? 8 A 0 = 2 > B 7 4 5 A L : 0 ? 8 A L
B @ 0 D 8 : 0 = 0 FreeBSD, 0 = 0 ; > 3 8 G = > NetFlow

Details

Info Sunday 14 March 2010 - 18:29:17 by

Vampyr`s House!