Netflow

> Netflow is een netwerk protocol die informatie verzameld en een toezicht houdt over het verkeersstroom van het netwerk . Netflow is ontwerpen door Cisco en werd in de 1996 beschikbaar gesteld op de Cisco routers. Netflow kan geconfigureerd worden om het verkeer van een interface in gaten te houden. Er is een mogelijkheid om alleen de binnenkomende en/of uitgaande verkeer op die interface te monitoren. In het document *nbarConfig.pdf* hebben het over Nbar gesproken, meer uitleg over de verschillen tussen Nbar en Netflow gaan we in een andere document bespreken. Met Netflow krijgen we een weergave van de volume, de afkomst en bestemming en hoeveel verkeer in het netwerk gegeneerd word door die pakketten.

Configure Netflow and verify config

1. Configure Netflow and Data Export

> Hier gaan we Netflow configureren en ook data export. Met data export kunnen we de opgenomen gegevens exporteren naar een externe analyzer.
>
> `root@graylogDebian: enable`
>
> `root@graylogDebian: configure terminal`
>
> Nu gaan we netflow configureren en ook aangeven naar welke adres de export gedaan moet worden en door welke port. We hebben een Grylog geconfigureerd om te gebruiken als de analyzer voor onze export. Dus zal de data geëxporteerd worden naar het adres van de Graylog(10.20.120.9).
>
> `root@graylogDebian: ip flow-export destnation*{ip-address|hostname}* udp-port`
>
> ```
> LGL-Router-C2900-3p(config)#ip flow-export des
> LGL-Router-C2900-3p(config)#ip flow-export destination 10.20.120.9 9996
> ```
>
> **Herhaal de vorige commando als je data export naar verschillende analyzers en/of via andere porten wild sturen.**
>
> `root@graylogDebian: ip flow-export vesion 9`
>
> Nu moeten we de interface ingeven waar de monitoring gebeurt moet worden.
>
> `root@graylogDebian: interface g0/1`
>
> ```
> LGL-Router-C2900-3p(config)#ip flow-export version 9
> LGL-Router-C2900-3p(config)#in
> LGL-Router-C2900-3p(config)#interface g0/1
> ```
>
> Het is nu tijd om in te geven of we het inkomende verkeer(ingress) of uitgaande verkeer(egress) op de interface zullen monitoren. We kunnen ook ervoor kiezen om beide te doen.
>
> `root@graylogDebian: ip flow {ingress|egress}`

```
LGL-Router-C2900-3p(config-if)#ip flow ingress
LGL-Router-C2900-3p(config-if)#ip flow eg
LGL-Router-C2900-3p(config-if)#ip flow egress
```

`root@graylogDebian: exit`

Herhaal de commmandos vanaf *root@graylogDebian: interface g0/1* **tot en met** `root@graylogDebian: exit` **om netflow te configuren op andere interfaces**

`root@graylogDebian: end`

2. Verify Netflow

We gaan nu controleren of Netflow goed geconfigureerd is en of data export in orde is.

1. Is Netflow enabled

Interface check

Eerste manier om dit te controleren is de interface, we controleren of de interface waarop we Netflow geconfigureerd hebben in orde is.

`root@graylogDebian: show ip interface`

```
LGL-Router-C2900-3p#show ip flow interface
GigabitEthernet0/1
  ip flow ingress
  ip flow egress
```

** Dit klopt, de configuraties gebeurde op g0/1 en het was zowel ingress en egress**

Cach flow

Nu we zeker weten dat de interface in orde is gaan we kijken of Netflow zelf operationeel is en vragen we een samenvatting van de Netflow statistieken. De ontleden van netflow samenvatting gaan we in de documenten ** verder ontleden

`root@graylogDebian: show ip cach flow`

```
LGL-Router-C2900-3p#show ip cache flow
IP packet size distribution (101517255 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .331 .098 .019 .031 .013 .006 .007 .005 .003 .007 .002 .002 .001 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .018 .020 .421 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  639 active, 3457 inactive, 6022429 added
  108612787 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 66824 bytes
  639 active, 1409 inactive, 6018552 added, 6018552 added to flow
  0 alloc failures, 1081 force free
  2 chunks, 86 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           1      0.0         1    44      0.0       0.0      15.5
TCP-FTP              1      0.0        35    75      0.0       2.9       1.4
TCP-WWW         241377      0.0        96   987      7.0       4.4       6.9
TCP-SMTP            25      0.0       761  1039      0.0       1.1       1.5
TCP-X                4      0.0         1    46      0.0       0.0       8.4
TCP-Frag            70      0.0         5   670      0.0       2.0      15.5
TCP-other      3889622      1.1        15   646     18.5       2.3      10.0
UDP-DNS         658692      0.1         1    78      0.2       0.1      15.5
UDP-NTP         101504      0.0         1    76      0.0       0.0      15.5
UDP-Frag             1      0.0         1   475      0.0       0.0      15.6
UDP-other      1125792      0.3        12   516      4.2      16.1      15.4
ICMP              4462      0.0       368    86      0.4     399.0      12.5
GRE                190      0.0       204   695      0.0      31.8      15.4
IP-other           239      0.0       194    82      0.0    1792.6       4.9
Total:         6021980      1.8        16   693     30.5       5.1      11.6
```

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/2         195.154.227.214 Gi0/1*        10.20.40.94     06 B903 A60A    39
Gi0/2         172.217.20.74   Gi0/1*        10.20.1.126     11 01BB FC28   418
Gi0/1         10.20.1.104     Gi0/2         67.27.150.254   06 C90C 0050   432
Gi0/1         10.20.1.104     Gi0/2         67.27.150.254   06 C902 0050   408
Gi0/2         209.206.58.50   Gi0/1*        10.20.40.92     11 1CB7 A39F     1
Gi0/2         40.101.12.114   Gi0/1*        10.20.1.119     06 01BB D577     1
Gi0/2         209.206.57.28   Gi0/1*        10.20.40.92     11 1CB7 A04F    39
Gi0/2         172.217.20.106  Gi0/1*        10.20.40.77     06 01BB 8005    42
Gi0/1         10.20.1.104     Gi0/2         8.247.210.126   06 C8FD 0050   232
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FF72 0035     1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/1         10.20.120.41    Gi0/2         212.83.232.101  06 D218 0050    21
Gi0/2         172.217.168.227 Gi0/1*        10.20.10.23     06 01BB EF00     7
Gi0/2         185.30.176.64   Gi0/1*        10.20.1.123     06 01BB C412    10
Gi0/2         185.30.176.64   Gi0/1*        10.20.1.123     06 01BB C411    13
Gi0/2         51.255.138.215  Gi0/1*        10.20.30.30     11 007B AF31     1
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FFB9 0035     1
Gi0/2         172.217.17.37   Gi0/1*        10.20.120.26    06 01BB F450    11
Gi0/1         10.20.10.23     Gi0/2         108.177.126.189 06 EF23 01BB     1
Gi0/2         54.183.120.66   Gi0/1*        10.20.30.19     06 01BB 95DC     1
Gi0/1         10.20.120.28    Gi0/2         74.125.143.189  11 F570 01BB   123
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FF9E 0035     1
Gi0/1         10.20.120.31    Gi0/2         86.105.244.3    06 E148 01BB     7
Di1           172.24.20.234   Gi0/1*        10.20.30.11     11 F187 00A1     1
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FF92 0035     1
Gi0/2         13.78.177.144   Gi0/1*        10.20.1.138     06 01BB F87A     9
Gi0/2         52.239.242.148  Gi0/1*        10.20.120.26    06 01BB F5E2     1
Gi0/2         185.162.29.42   Gi0/1*        10.20.1.143     06 01BB FECC     4
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FFE5 0035     1
Gi0/1         10.20.10.4      Gi0/2         178.32.206.33   06 F571 01BB   126
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FFD1 0035     1
Gi0/1         10.20.40.94     Gi0/2         5.79.77.52      06 EDA6 CB6D  4523
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FFCE 0035     1
```

gedatailleerde Cach flow

> Met deze commando krijg je een meer gedatailleerde sammenvatting van de netflow statestieken. We krijgen bijvoorbeeld ook poortnr , nexthop etc.
>
> `root@graylogDebian: show ip cach verbose flow`

```
LGL-Router-C2900-3p#show ip cach verbose flow
IP packet size distribution (103095658 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .330 .097 .019 .031 .013 .006 .007 .005 .003 .007 .002 .002 .001 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .018 .020 .423 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  723 active, 3373 inactive, 6063057 added
  109299007 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 66824 bytes
  723 active, 1325 inactive, 6059180 added, 6059180 added to flow
  0 alloc failures, 1081 force free
  2 chunks, 86 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           1      0.0         1    44      0.0       0.0      15.5
TCP-FTP              1      0.0        35    75      0.0       2.9       1.4
TCP-WWW         244132      0.0        97   987      7.1       4.4       6.9
TCP-SMTP            31      0.0       614  1038      0.0       0.9       2.8
TCP-X                4      0.0         1    46      0.0       0.0       8.4
TCP-Frag            70      0.0         5   670      0.0       2.0      15.5
TCP-other      3917576      1.1        15   648     18.8       2.3      10.0
UDP-DNS         663546      0.2         1    78      0.2       0.1      15.5
UDP-NTP         101714      0.0         1    76      0.0       0.0      15.5
UDP-Frag             1      0.0         1   475      0.0       0.0      15.6
UDP-other      1130506      0.3        12   518      4.2      16.1      15.4
ICMP              4480      0.0       367    86      0.4     397.9      12.5
GRE                190      0.0       204   695      0.0      31.8      15.4
IP-other           239      0.0       194    82      0.0    1792.6       4.9
Total:         6062491      1.8        16   695     31.0       5.1      11.6
```

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                   Port Msk AS   NextHop             B/Pk  Active
Gi0/1         10.20.30.23     Gi0/2         85.93.20.46     06 02  1A       5
0D3D /24 0                    1C10 /0  0    81.82.192.1           435     1.2

Gi0/2         195.154.227.214 Gi0/1*        10.20.40.94     06 00  18    2575
B903 /0  0                    A60A /24 0    192.168.2.2          1287   924.7
FFlags: 01

Gi0/2         172.217.17.110  Gi0/1*        10.20.120.53    11 00  10      88
01BB /0  0                    D00C /24 0    192.168.2.2           471    95.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                   Port Msk AS   NextHop             B/Pk  Active
FFlags: 01

Gi0/2         85.93.20.46     Gi0/1*        10.20.30.23     06 00  10       6
1C10 /0  0                    0D3D /24 0    192.168.2.2           40     3.1
FFlags: 01

Gi0/2         85.93.20.46     Gi0/1*        10.20.30.23     06 02  1A       7
1C10 /0  0                    0D3D /24 0    192.168.2.2          237     3.2
FFlags: 01

Gi0/2         172.217.17.37   Gi0/1*        10.20.90.23     06 00  10       1
01BB /0  0                    E6C5 /24 0    192.168.2.2           52     0.0
FFlags: 01

Gi0/2         209.206.58.50   Gi0/1*        10.20.40.92     11 00  10       1
1CB7 /0  0                    A39F /24 0    192.168.2.2           74     0.0
FFlags: 01

Gi0/2         209.206.58.50   Gi0/1*        10.20.40.77     11 00  10       1
1CB7 /0  0                    A353 /24 0    192.168.2.2           74     0.0
FFlags: 01
```

2. Data Export Controle

Nu moet er een controle gebeuren om te controleren of data Export goed geconfigureerd is. Met de volgende commando krijgen we een samenvatting over de data export. We kunnen dan zien naar waar het verstuurd word welke poortnr, versie, hoeveel pakketten verstuurd of gedropped etc.

`root@graylogDebian: show ip flow export`

```
LGL-Router-C2900-3p#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  10.20.120.9 (9996)
  Version 9 flow records
  11024880 flows exported in 380936 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Deze Document is om voor het configureren en controleren van de netflow. De betekenis van de weergaven zal in het document *netflowAnalyze.pdf* **uitgelegd worden in met meer details**