Analyze Netflow Statistics

> In deze document gaan we de verschillende delen van de show commando's die we het document *netflowConfig.pdf*gebruikt hebben doorlopen en uitleggen. Hierdoor horen we een betere zicht te krijgen van onze verkeer en een idee van de oorzaak van de problemen in onze netwerk. Daarna zullen we zien hoe we de show commando's kunnen aanpassen en filteren om meer gefocust informaties kunnen krijgen.

Analyzing the Show commands

1. Show ip cach flow

1.Packet size Distrubution

> Dit is de eerste deel van de samenvatting. Hier krijgen we informatie over de Groottes van de verschillende IP-pakketten die door de interface gaan. De bovenste regel vertelt ons hoeveel pakketten we in totaal hebben. Er zijn in totaal 109 miljoen pakketten door onze interface gekomen.

```
IP packet size distribution (109613635 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .330 .096 .018 .030 .012 .006 .007 .005 .003 .007 .002 .002 .001 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .019 .020 .425 .000 .000 .000 .000 .000 .000
```

> Middelste regel geeft ons een overzicht met van de verschillende groottes. De verdeling heeft een toename van 32 Byte.

```
IP packet size distribution (109613635 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .330 .096 .018 .030 .012 .006 .007 .005 .003 .007 .002 .002 .001 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .019 .020 .425 .000 .000 .000 .000 .000 .000
```

> In de laatste regel zien we de verdeling van pakketten in percentage. De eerste pakket die we tegen komen is 64 Byte. Een IP Pakket heeft een minimum grootte van 64 Byte. Er zijn 33% bij 64 Byte en de meeste aantal pakketten zijn 1536 Byte groot met een percentage van 42%.

```
IP packet size distribution (109613635 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .330 .096 .018 .030 .012 .006 .007 .005 .003 .007 .002 .002 .001 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .019 .020 .425 .000 .000 .000 .000 .000 .000
```

2.Protocols

> Helemaal links heb je een overzicht van de protocollen die door die interface gekomen is. Deze lijst is natuurlijk een verdeling van de 109 Miljoenen pakketten

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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	251801	0.0	95	986	7.2	4.4	6.9
TCP-SMTP	39	0.0	496	1031	0.0	0.8	3.3
TCP-X	4	0.0	1	46	0.0	0.0	8.4
TCP-Frag	86	0.0	4	700	0.0	2.4	15.5
TCP-other	4119908	1.2	16	657	20.4	2.4	10.0
UDP-DNS	690593	0.2	1	78	0.2	0.1	15.5
UDP-NTP	103896	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	1170419	0.3	12	528	4.5	16.2	15.4
ICMP	4618	0.0	362	86	0.5	393.6	12.5
GRE	197	0.0	646	477	0.0	77.0	15.2
IP-other	243	0.0	194	82	0.0	1792.7	4.9
Total:	6341807	1.9	17	698	33.0	5.1	11.5

Total Flows de totaal aantal keer die protocol door de interface gekomen is sinds de laatste statistieken verwijderd werden. *Flow/sec* Hoe vaak die protocol per seconde door de interface komt. *Packets/Flow* Gemiddelde pakketten die er elke keer zijn wanneer deze protocol actief is.

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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	251801	0.0	95	986	7.2	4.4	6.9
TCP-SMTP	39	0.0	496	1031	0.0	0.8	3.3
TCP-X	4	0.0	1	46	0.0	0.0	8.4
TCP-Frag	86	0.0	4	700	0.0	2.4	15.5
TCP-other	4119908	1.2	16	657	20.4	2.4	10.0
UDP-DNS	690593	0.2	1	78	0.2	0.1	15.5
UDP-NTP	103896	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	1170419	0.3	12	528	4.5	16.2	15.4
ICMP	4618	0.0	362	86	0.5	393.6	12.5
GRE	197	0.0	646	477	0.0	77.0	15.2
IP-other	243	0.0	194	82	0.0	1792.7	4.9
Total:	6341807	1.9	17	698	33.0	5.1	11.5

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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	251801	0.0	95	986	7.2	4.4	6.9
TCP-SMTP	39	0.0	496	1031	0.0	0.8	3.3
TCP-X	4	0.0	1	46	0.0	0.0	8.4
TCP-Frag	86	0.0	4	700	0.0	2.4	15.5
TCP-other	4119908	1.2	16	657	20.4	2.4	10.0
UDP-DNS	690593	0.2	1	78	0.2	0.1	15.5
UDP-NTP	103896	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	1170419	0.3	12	528	4.5	16.2	15.4
ICMP	4618	0.0	362	86	0.5	393.6	12.5
GRE	197	0.0	646	477	0.0	77.0	15.2
IP-other	243	0.0	194	82	0.0	1792.7	4.9
Total:	6341807	1.9	17	698	33.0	5.1	11.5

De twee laatste velden bereken hoeveel sec een bepaalde pakket actief was tot ze inactief werden.

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /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	251801	0.0	95	986	7.2	4.4	6.9
TCP-SMTP	39	0.0	496	1031	0.0	0.8	3.3
TCP-X	4	0.0	1	46	0.0	0.0	8.4
TCP-Frag	86	0.0	4	700	0.0	2.4	15.5
TCP-other	4119908	1.2	16	657	20.4	2.4	10.0
UDP-DNS	690593	0.2	1	78	0.2	0.1	15.5
UDP-NTP	103896	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	1170419	0.3	12	528	4.5	16.2	15.4
ICMP	4618	0.0	362	86	0.5	393.6	12.5
GRE	197	0.0	646	477	0.0	77.0	15.2
IP-other	243	0.0	194	82	0.0	1792.7	4.9
Total:	6341807	1.9	17	698	33.0	5.1	11.5

3.Senders, Receivers and Destinations

SrcIf Is de Interface die het pakket ontvangen heeft. *SrcIPaddress* IP-adres van het toestel die het pakket verzonden heeft

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/2	13.69.158.96	Gi0/1*	10.20.1.104	06	01BB	CEE4	1
Gi0/2	209.206.58.50	Gi0/1*	10.20.40.92	11	1CB7	A39F	1
Gi0/1	10.20.40.95	Gi0/2	209.206.57.28	11	AD3E	1CB7	16
Gi0/1	10.20.1.211	Gi0/2	172.217.218.189	11	D0FF	01BB	139
Gi0/2	108.177.126.189	Gi0/1*	10.20.1.211	11	01BB	C1CB	62
Gi0/1	10.20.30.3	Null	8.8.8.8	11	FF7F	0035	1
Gi0/1	10.20.120.28	Gi0/2	192.0.76.3	06	D3CA	01BB	1
Gi0/2	172.217.20.110	Gi0/1*	10.20.120.26	11	01BB	C6BF	22
Gi0/2	172.217.20.110	Gi0/1*	10.20.120.36	06	01BB	F093	15
Gi0/2	172.217.20.106	Gi0/1*	10.20.120.36	06	01BB	F091	20

DstIf Interface die het pakket verstuurd heeft. *DstIPaddress* IP-adres voor de ontvanger.

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi0/2	13.69.158.96	Gi0/1*	10.20.1.104	06	01BB	CEE4	1
Gi0/2	209.206.58.50	Gi0/1*	10.20.40.92	11	1CB7	A39F	1
Gi0/1	10.20.40.95	Gi0/2	209.206.57.28	11	AD3E	1CB7	16
Gi0/1	10.20.1.211	Gi0/2	172.217.218.189	11	D0FF	01BB	139
Gi0/2	108.177.126.189	Gi0/1*	10.20.1.211	11	01BB	C1CB	62
Gi0/1	10.20.30.3	Null	8.8.8.8	11	FF7F	0035	1
Gi0/1	10.20.120.28	Gi0/2	192.0.76.3	06	D3CA	01BB	1
Gi0/2	172.217.20.110	Gi0/1*	10.20.120.26	11	01BB	C6BF	22
Gi0/2	172.217.20.110	Gi0/1*	10.20.120.36	06	01BB	F093	15
Gi0/2	172.217.20.106	Gi0/1*	10.20.120.36	06	01BB	F091	20

Pr de IP-protocol poortnummer in de RFC 1340, poortnummer is in hexadecimaal getal. *SrcP* Poortnummer van de verzender van deze protocol. *DstP* de ontvanger poortnummer voor deze protocol.

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/2         13.69.158.96    Gi0/1*        10.20.1.104     06 01BB CEE4     1
Gi0/2         209.206.58.50   Gi0/1*        10.20.40.92     11 1CB7 A39F     1
Gi0/1         10.20.40.95     Gi0/2         209.206.57.28   11 AD3E 1CB7    16
Gi0/1         10.20.1.211     Gi0/2         172.217.218.189 11 D0FF 01BB   139
Gi0/2         108.177.126.189 Gi0/1*        10.20.1.211     11 01BB C1CB    62
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FF7F 0035     1
Gi0/1         10.20.120.28    Gi0/2         192.0.76.3      06 D3CA 01BB     1
Gi0/2         172.217.20.110  Gi0/1*        10.20.120.26    11 01BB C6BF    22
Gi0/2         172.217.20.110  Gi0/1*        10.20.120.36    06 01BB F093    15
Gi0/2         172.217.20.106  Gi0/1*        10.20.120.36    06 01BB F091    20
```

Pkts de Hoeveelheid pakketten die door de verkeersstroom gestroomd is.


```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/2         13.69.158.96    Gi0/1*        10.20.1.104     06 01BB CEE4     1
Gi0/2         209.206.58.50   Gi0/1*        10.20.40.92     11 1CB7 A39F     1
Gi0/1         10.20.40.95     Gi0/2         209.206.57.28   11 AD3E 1CB7    16
Gi0/1         10.20.1.211     Gi0/2         172.217.218.189 11 D0FF 01BB   139
Gi0/2         108.177.126.189 Gi0/1*        10.20.1.211     11 01BB C1CB    62
Gi0/1         10.20.30.3      Null          8.8.8.8         11 FF7F 0035     1
Gi0/1         10.20.120.28    Gi0/2         192.0.76.3      06 D3CA 01BB     1
Gi0/2         172.217.20.110  Gi0/1*        10.20.120.26    11 01BB C6BF    22
Gi0/2         172.217.20.110  Gi0/1*        10.20.120.36    06 01BB F093    15
Gi0/2         172.217.20.106  Gi0/1*        10.20.120.36    06 01BB F091    20
```


Samenvatting

Met de nieuwe informatie die we hebben kunnen we nu de output een beetje beter begrijpen, dus zal ik de eerste regel in normale mensen taal schrijven.

Er is **1** pakket van **HTTPS** verstuurd van de interface **Gi0/1** met IP-adres **13.69.158.96** naar de **01BB**(443) via de door de interface **Gi0/2** met adres **10.20.1.104**.

Met andere woorden iemand gaat op internet door de interface **Gi0/2**.


```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/2         13.69.158.96    Gi0/1*        10.20.1.104     06 01BB CEE4     1
```


2. Show ip cach verbose flow

De output van de show verbose commando is, een beetje hetzelfde als de eerste. De verbose heeft een paar extra informaties die de eerste optie niet heeft. De poort is leesbaarder omdat het in cijfer is **8865**. Er is een veld MSK voor de subnet mask van het netwerk **/24**. Ten laatste is eer en veld *Next hop* voor volgende Hop-adres **10.20.40.95**.

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs   Pkts
Port Msk AS                   Port Msk AS   NextHop              B/Pk  Active
Gi0/2         47.74.247.66    Gi0/1*        10.20.40.95     06 00  18        6
AD9B /0  0                    8865 /24 0    192.168.2.2            43     16.1
FFlags: 01
```

Filtering the Show commands

Nu gaan we een paar command doen om meer informatie te krijgen. We gaan de gegevens filteren om de antwoorden te vinden op bepaalde vragen.

1. Show top 10

Nu gaan we zien welke protocollen veel verkeer versturen op het netwerk . Om dit te doen moeten eerst een paar configuraties doen.

```
root@graylogDebian: config terminal
```

```
root@graylogDebian: ip flow-top-talkers
```

```
root@graylogDebian: top 10
```

```
root@graylogDebian: sort-by bytes
```

```
LGL-Router-C2900-3p(config)#ip flow-top-talkers
LGL-Router-C2900-3p(config-flow-top-talkers)#top 10
LGL-Router-C2900-3p(config-flow-top-talkers)#sor
LGL-Router-C2900-3p(config-flow-top-talkers)#sort-by by
LGL-Router-C2900-3p(config-flow-top-talkers)#sort-by bytes
```

```
root@graylogDebian: show ip flow top-takers
```

```
LGL-Router-C2900-3p#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Gi0/2         208.117.238.84  Gi0/1*        10.20.10.17     06 01BB E3EE  2754K
Gi0/2         208.117.238.15  Gi0/1*        10.20.40.140    06 01BB DD87  2691K
Gi0/2         2.17.107.33     Gi0/1*        10.20.120.48    06 0050 D0A0   276K
Gi0/2         2.18.175.102    Gi0/1*        10.20.10.27     06 01BB F46D   171K
Gi0/2         172.217.20.78   Gi0/1*        10.20.40.140    06 01BB DD00   125K
Gi0/1         10.20.40.140    Gi0/2         208.117.238.15  06 DD87 01BB    83K
Gi0/1         10.20.10.17     Gi0/2         208.117.238.84  06 E3EE 01BB    83K
Gi0/1         10.20.1.116     Gi0/2         40.74.32.146    06 EB14 01BB    78K
Gi0/1         10.20.40.140    Gi0/2         172.217.20.78   06 DD00 01BB    71K
Gi0/1         10.20.10.27     Gi0/2         2.18.175.102    06 F474 01BB    67K
10 of 10 top talkers shown. 375 flows processed.
```

Wat ik hieruit kan lezen is dat het meeste pakketten via port **01BB**(443) dus HTTPS wat geen probleem is. De tweede meeste is **0050**(80)HTTP. Meeste pakketten zijn zijn van mensen die op internet gaan dit is geen probleem.

2. Show top 20

In de top 10 hebben we niets verdachts of erg gezien dus Nu top 20.

```
root@graylogDebian: config terminal
```

```
root@graylogDebian: ip flow-top-talkers
```

```
root@graylogDebian: top 20
```

```
root@graylogDebian: sort-by bytes
```

```
root@graylogDebian: show ip flow top-takers
```

Nu komen we een poort **0FE6**(4070)tegen. Het protocol die aan deze poort verbonden is heet *tripe* **Trival IP Encription(TrIPE)**, dit is een Amazone service die stremming connecties maak met Spotify. Dit ga we moeten oplossen.

```
LGL-Router-C2900-3p#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Gi0/2         193.182.8.115   Gi0/1*        10.20.40.76     06 01BB BA5D   19M
Gi0/2         208.117.238.77  Gi0/1*        10.20.40.76     06 01BB 910B   13M
Gi0/2         35.186.224.53   Gi0/1*        10.20.40.76     06 01BB C122 1701K
Gi0/2         208.117.238.15  Gi0/1*        10.20.40.140    06 01BB DE30 1407K
Gi0/2         104.199.65.73   Gi0/1*        10.20.40.76     06 0FE6 948F  695K
Gi0/1         10.20.40.76     Gi0/2         193.182.8.115   06 BA5D 01BB  398K
Gi0/2         172.217.17.150  Gi0/1*        10.20.40.140    06 01BB DE22  288K
Gi0/1         10.20.40.76     Gi0/2         208.117.238.77  06 910B 01BB  260K
Gi0/2         172.217.20.78   Gi0/1*        10.20.40.140    06 01BB DDC7  190K
Gi0/1         10.20.40.76     Gi0/2         35.186.224.53   06 C122 01BB  143K
Gi0/1         10.20.40.76     Gi0/2         104.199.65.73   06 948F 0FE6   88K
Gi0/2         208.117.238.82  Gi0/1*        10.20.40.140    06 01BB DE28   79K
Gi0/2         208.117.238.82  Gi0/1*        10.20.40.140    06 01BB DE27   77K
Gi0/2         208.117.238.15  Gi0/1*        10.20.40.140    06 01BB DE2F   69K
Gi0/1         10.20.40.140    Gi0/2         172.217.20.78   06 DDC7 01BB   69K
Gi0/2         8.8.8.8         Gi0/1*        10.20.1.103     01 0000 0000   68K
Gi0/2         8.8.8.8         Gi0/1*        10.20.40.220    01 0000 0000   68K
Gi0/1         10.20.40.220    Gi0/2         8.8.8.8         01 0000 0800   63K
Gi0/1         10.20.1.103     Gi0/2         8.8.8.8         01 0000 0800   63K
Gi0/2         2.20.202.106    Gi0/1*        10.20.1.84      06 01BB F427   27K
```

De tweede poort die ik opgemerkt heb, is de poort **0800**(2048). Het is een port die gebruikt wordt door Web cach Control Protocol van Cisco, dit is geen probleem. Deze poort wordt gebruik door Camarades die zorgt voor portfowarding en dls-monitor van Nmap. Deze twee services zijn geen Probleem, ik heb op meerder site gezien dat poort 2048 gevaarlijk kan zijn omdat er een threat genaamd *Shiva/spider* op die poort kan luister naar configuraties van Telnet.

```
LGL-Router-C2900-3p#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Gi0/2         193.182.8.115   Gi0/1*        10.20.40.76     06 01BB BA5D   19M
Gi0/2         208.117.238.77  Gi0/1*        10.20.40.76     06 01BB 910B   13M
Gi0/2         35.186.224.53   Gi0/1*        10.20.40.76     06 01BB C122 1701K
Gi0/2         208.117.238.15  Gi0/1*        10.20.40.140    06 01BB DE30 1407K
Gi0/2         104.199.65.73   Gi0/1*        10.20.40.76     06 0FE6 948F  695K
Gi0/1         10.20.40.76     Gi0/2         193.182.8.115   06 BA5D 01BB  398K
Gi0/2         172.217.17.150  Gi0/1*        10.20.40.140    06 01BB DE22  288K
Gi0/1         10.20.40.76     Gi0/2         208.117.238.77  06 910B 01BB  260K
Gi0/2         172.217.20.78   Gi0/1*        10.20.40.140    06 01BB DDC7  190K
Gi0/1         10.20.40.76     Gi0/2         35.186.224.53   06 C122 01BB  143K
Gi0/1         10.20.40.76     Gi0/2         104.199.65.73   06 948F 0FE6   88K
Gi0/2         208.117.238.82  Gi0/1*        10.20.40.140    06 01BB DE28   79K
Gi0/2         208.117.238.82  Gi0/1*        10.20.40.140    06 01BB DE27   77K
Gi0/2         208.117.238.15  Gi0/1*        10.20.40.140    06 01BB DE2F   69K
Gi0/1         10.20.40.140    Gi0/2         172.217.20.78   06 DDC7 01BB   69K
Gi0/2         8.8.8.8         Gi0/1*        10.20.1.103     01 0000 0000   68K
Gi0/2         8.8.8.8         Gi0/1*        10.20.40.220    01 0000 0000   68K
Gi0/1         10.20.40.220    Gi0/2         8.8.8.8         01 0000 0800   63K
Gi0/1         10.20.1.103     Gi0/2         8.8.8.8         01 0000 0800   63K
Gi0/2         2.20.202.106    Gi0/1*        10.20.1.84      06 01BB F427   27K
```

Poort **01BB**(443) komt veel voor dus ik wil de top 20 zien zonder de poort 443.

```
root@graylogDebian: show ip flow top-takers | exclude 001BB
```

> Dit ziet er ook uit. Poort **03E1**(993) word gebruikt door IMAP, en poort **E09C**(57500) wordt gebruikt door *Xsan Filesystem Access* van Apple.

```
LGL-Router-C2900-3p#show ip flow top-talkers | exclude 01BB

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Gi0/2         74.125.143.108  Gi0/1*        10.20.40.140    06 03E1 E09C  1904K
Gi0/1         10.20.40.140    Gi0/2         74.125.143.108  06 E09C 03E1   320K
Gi0/2         8.8.8.8         Gi0/1*        10.20.1.103     01 0000 0000    89K
Gi0/2         8.8.8.8         Gi0/1*        10.20.40.220    01 0000 0000    89K
Gi0/1         10.20.40.220    Gi0/2         8.8.8.8         01 0000 0800    84K
Gi0/1         10.20.1.103     Gi0/2         8.8.8.8         01 0000 0800    84K
220 of 20 top talkers shown. 577 flows processed.
```