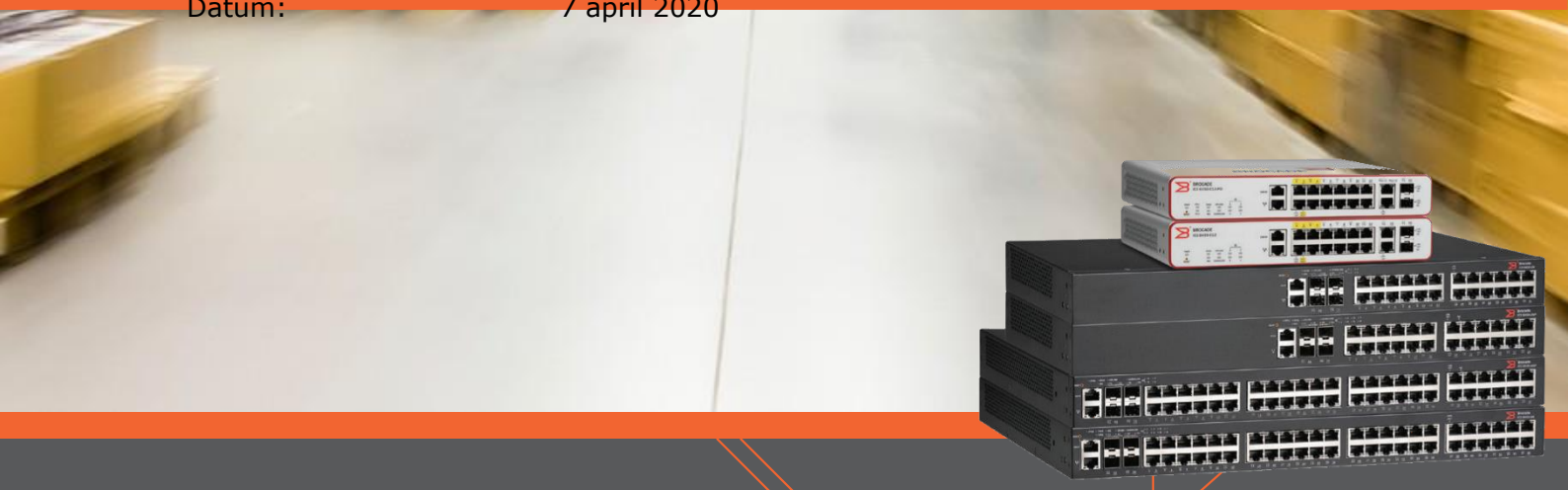
Alcadis
confidence in connectivity

ICX TECHNOTE - PORT MIRROR V1.0

Ruckus ICX configuratie – Port mirror

Versie: 1.0
Auteur: Herwin de Rijke
Datum: 7 april 2020



Inhoud

1 Inleiding 2

1.1 DOELSTELLING 2
1.2 BEOOGD PUBLIEK 2
1.3 VOORKENNIS/BENODIGDHEDEN 2

2 Port mirroring 3

2.1 STANDAARD WAARDEN 4
2.2 ENKELE POORT MONITOREN 5
2.3 MEERDERE POORTEN MONITOREN 5
2.4 MONITOREN INPUT EN OUTPUT VERKEER 6
2.5 MONITOREN VAN EEN LAG 6

3 Wireshark 7

3.1 FILTERS 7
3.2 APPLY AS FILTER FUNCTIE 9
3.3 CONVERSATION 9
3.4 COLORING RULES 10
3.5 WIRESHARK TOOLS 11

1 Inleiding

In dit document wordt beschreven op welke manier port mirroring geconfigureerd kan worden op een ICX switch.
Daarnaast worden er enkele voorbeelden van analyse mogelijkheden in het programma Wireshark getoond.

De instructies die in dit document gegeven worden zijn op basis van firmware versie Version 08.0.90. Wij raden aan om uw switch te upgraden naar deze versie of hoger. Mogelijk zijn in andere versies als gebruikte versies bepaalde functies niet beschikbaar of is de werking anders.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met de manier waarop port mirroring op een Ruckus ICX switch kan worden geconfigureerd.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel die een Ruckus ICX switch willen configureren om gebruik te maken van port mirroring.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- Basiskennis van IPv4
- Basiskennis Ruckus ICX Command Line
- Basiskennis Wireshark

2 Port mirroring

Een switch stuurt standaard verkeer dat aan een client geadresseerd is alleen naar de switch poort waarop het MAC adres van deze client geleerd is. Om dit verkeer te kunnen bekijken vanaf een andere poort moet dit apart worden geconfigureerd.
Op de switch poort waar een device op aangesloten is zul je standaard alleen unicast verkeer zien gericht aan het device en broadcast verkeer.
Om op deze poort ook het verkeer dat gericht is op andere poorten te kunnen zien kan op de meeste managed switches port mirroring worden ingesteld.

Bij de Ruckus ICX switch zijn hiervoor twee typen poorten gedefinieerd.
Monitor poorten zijn poorten waarop devices zijn aangesloten waarvan het verkeer gekopieerd wordt. Mirror poorten zijn de poorten waar het verkeer naartoe wordt gekopieerd. Op deze poort wordt het capture device, bijvoorbeeld een laptop met wireshark aangesloten.

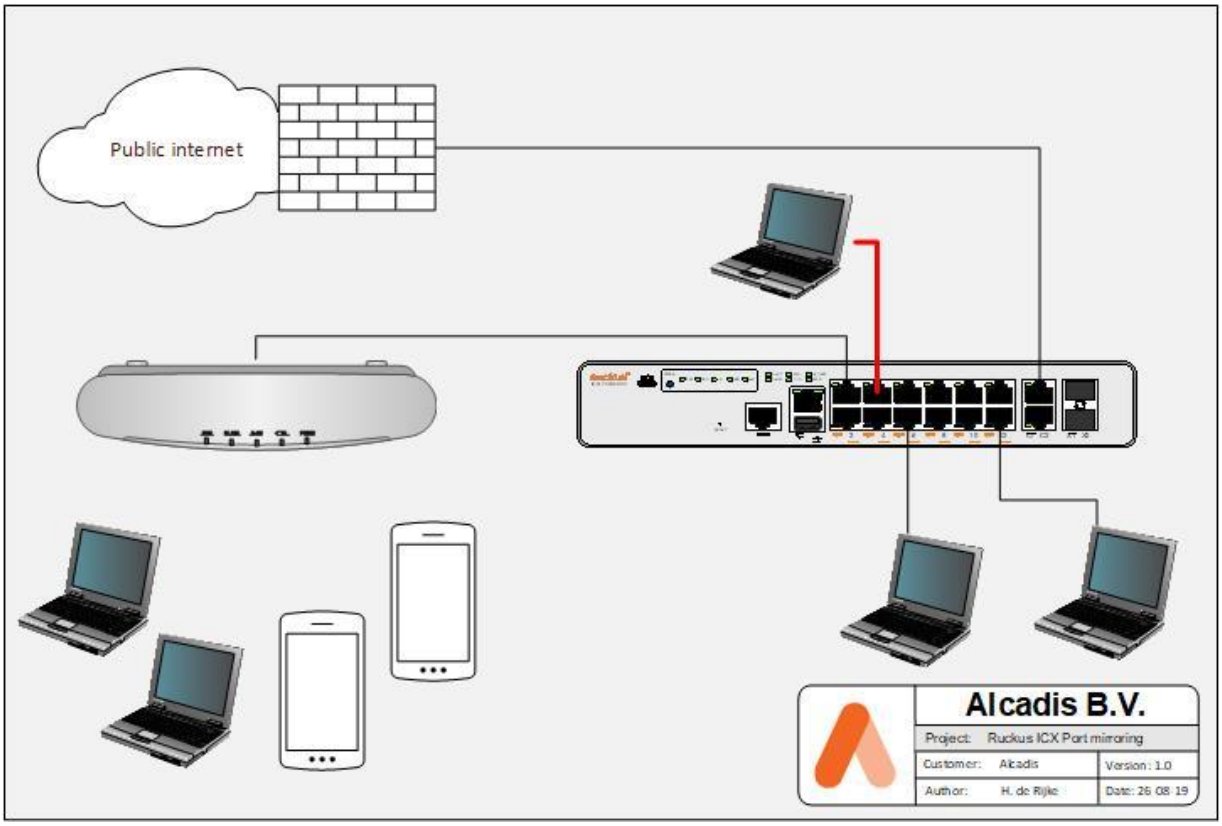
Daarnaast kan er onderscheid gemaakt worden tussen ingress en egress verkeer. Ingress verkeer is al het inkomende verkeer op een poort, egress is al het uitgaande verkeer van een poort. Er is voor elk type poort een beperking in het maximaal aantal beschikbare poorten per region.

Port type	Maximum supported
Ingress mirror port	1 per port region
Egress mirror port	1 per port region
Ingress monitoring port	No limit
Egress monitoring port	8 per port region

- Het is mogelijk meerdere monitoring poorten in te stellen in combinatie met 1 mirror poort
- Het is mogelijk om al het ingress verkeer te configureren op een andere mirror poort dan het egress verkeer
- Het is niet mogelijk meerdere mirror poorten in te stellen die zowel ingress als egress verkeer bevatten.

In onderstaand voorbeeld is aangegeven welke foutmelding wordt weergegeven als je probeert in dezelfde region meerdere poorten in te stellen voor ingress of egress verkeer.

```
ICX7150(config)#show mirror
Mirror port 1/1/11
  Input monitoring      : (U1/M1)   7   9
  Output monitoring     : (U1/M1)   7   9
ICX7150(config)#mirror ethernet 1/1/8
Error - Inbound mirror port 1/1/11 is already active on this region.
Error - Outbound mirror port 1/1/11 is already active on this region.
```



2.1 Standaard waarden

In een standaard configuratie staat port mirroring niet ingesteld. De poort waar de laptop met wireshark op zit aangesloten zit, gedraagt zich precies zoals elke andere poort. Mocht er toch een port mirror actief zijn en je wilt deze uitschakelen dan kan dit met onderstaand commando. Let op dat voor elke poort een apart commando moet wordt ingevoerd.

```
ICX7150(config)#show mirror
Mirror port 1/1/6
  Input monitoring      : None
  Output monitoring     : (U1/M2)   1
Mirror port 1/1/12
  Input monitoring      : (U1/M2)   1
  Output monitoring     : None
ICX7150(config)#no mirror ethernet 1/1/12
ICX7150(config)#no mirror ethernet 1/1/6
```

2.2 Enkele poort monitoren

In onderstaand voorbeeld is op poort 1/1/1 een laptop aangesloten en op poort 1/1/3 een accesspoint. Door al het verkeer dat van en naar de switchpoort waarop het accesspoint aangesloten is te kopiëren naar de switchpoort waarop een laptop aangesloten is; kan al het verkeer van de wireless clients dat door het accesspoint gebridged wordt, geanalyseerd worden.

```
ICX7150#conf t
ICX7150(config)#mirror ethernet 1/1/3
ICX7150(config)#show mirror
Mirror port 1/1/3
  Input monitoring      : None
  Output monitoring     : None
ICX7150(config)#interface ethernet 1/1/1
ICX7150(config-if-e1000-1/1/1)#monitor ?
  both       Both incoming and outgoing packets
  ethernet   Specify mirror port to use
  input      Incoming packets
  output     Outgoing packets
  profile    select monitor profile
ICX7150(config-if-e1000-1/1/1)#monitor ethernet 1/1/3 both
ICX7150 (config-if-e1000-1/1/1)#exit
ICX7150 (config)#exit
ICX7150#show mirror
Mirror port 1/1/3
  Input monitoring      : (U1/M1)   1
  Output monitoring     : (U1/M1)   1
```

2.3 Meerdere poorten monitoren

In dit voorbeeld wordt al het input en output verkeer van poorten 1/1/6 en 1/1/12 naar poort 1/1/3 gekopieerd.

```
ICX7150#conf t
ICX7150(config)#mirror ethernet 1/1/3
ICX7150(config)#show mirror
Mirror port 1/1/3
  Input monitoring      : None
  Output monitoring     : None
ICX7150(config)#interface ethernet 1/1/6
ICX7150(config-if-e1000-1/1/1)#monitor ethernet 1/1/3 both
ICX7150 (config-if-e1000-1/1/6)#exit
ICX7150(config)#interface ethernet 1/1/12
ICX7150(config-if-e1000-1/1/12)#monitor ethernet 1/1/3 both
ICX7150 (config)#exit
ICX7150#show mirror
Mirror port 1/1/3
  Input monitoring      : (U1/M1)   6  12
  Output monitoring     : (U1/M1)   6  12
```

2.4 Monitoren input en output verkeer

In sommige situaties is het handig om alleen het verkeer dat naar een specifieke poort gestuurd wordt te onderzoeken of alleen het verkeer dat daarvan afkomstig is. Denk hierbij aan een uplink poort waarbij je bijvoorbeeld het DHCP verkeer richting server wilt onderzoeken of alleen het verkeer dat vanaf de server richting clients gaat. In onderstaand voorbeeld wordt het inkomende verkeer van uplink poort 1/2/1 naar een laptop met wireshark gestuurd die op poort 1/1/12 aangesloten is. Het uitgaande verkeer van de uplink poort wordt naar een andere laptop met wireshark op poort 1/1/6 gestuurd.

```
ICX7150#conf t
ICX7150 (config)#mirror ethernet 1/1/12 input
ICX7150 (config)#mirror ethernet 1/1/6 output
ICX7150 (config)#show mirror
Mirror port 1/1/6
  Input monitoring      : None
  Output monitoring     : None
Mirror port 1/1/12
  Input monitoring      : None
  Output monitoring     : None
ICX7150 (config)# interface ethernet 1/2/1
ICX7150 (config-if-e1000-1/2/1)#monitor ethernet 1/1/12 input
ICX7150 (config-if-e1000-1/2/1)#monitor ethernet 1/1/6 output
SSH@ALCLAB-SER-SW007(config-if-e1000-1/2/1)#show mirror
Mirror port 1/1/6
  Input monitoring      : None
  Output monitoring     : (U1/M2)    1
Mirror port 1/1/12
  Input monitoring      : (U1/M2)    1
  Output monitoring     : None
```

2.5 Monitoren van een LAG

Het is ook mogelijk om het verkeer van een LAG te monitoren, bijvoorbeeld als je inzicht wilt krijgen in het verkeer tussen een MER en een SER. Hier moet uiteraard wel rekening worden gehouden met de capaciteit van de mirror en monitor poort. Als er meer verkeer over de LAG gaat dan de capaciteit van de mirror poort is dan zal de packet capture niet de juiste informatie weergeven.

```
ICX7150#conf t
ICX7150(config)#mirror ethernet 1/1/1
ICX7150(config)#show mirror
Mirror port 1/1/1
  Input monitoring      : None
  Output monitoring     : None
ICX7150(config)#interface lag 1
ICX7150(config-lag-if-lg1)#monitor ethernet 1/1/3 both
ICX7150 (config-lag-if-lg1)#exit
ICX7150 (config)#exit
ICX7150#show mirror
Mirror port 1/1/1
  Input monitoring      : (U1/M3)    1    2
  Input monitoring      : (LAG)      1
  Output monitoring     : (U1/M3)    1    2
  Output monitoring     : (LAG)      1
ICX7150#
```

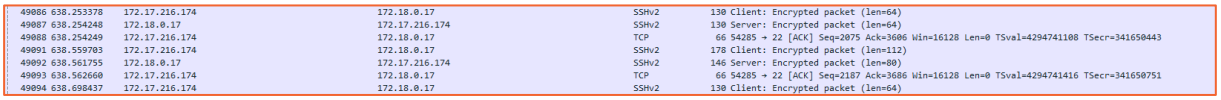
3 Wireshark

Het doel van een mirror is het kopiëren van het verkeer dat over een verbinding gaat. Om dit verkeer vervolgens te analyseren maak je gebruik van het programma Wireshark. In dit hoofdstuk geven we een aantal voorbeelden van filters die gebruikt kunnen worden de verzamelde pakketten te filteren. Op deze manier kan op eenvoudige wijze verkeer van specifieke clients of van een specifiek type worden onderzocht.
Daarnaast geven we nog een aantal voorbeelden van verdere gereedschappen die het programma biedt om de pakketten te onderzoeken

3.1 Filters

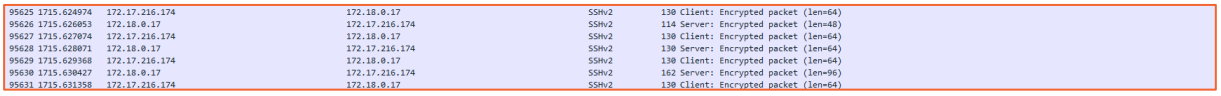
Als je al het verkeer afkomstig van en gericht aan een specifiek MAC adres wilt onderzoeken kun je dat doen met onderstaand filter:

filter
eth.addr == 24:79:2a24:0e:d0



Om verkeer afkomstig van en gericht aan een specifiek IP adres te onderzoeken gebruik je onderstaand filter:

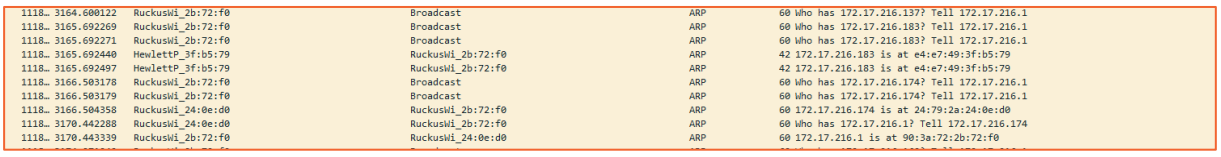
filter:
ip.addr == 172.17.216.174



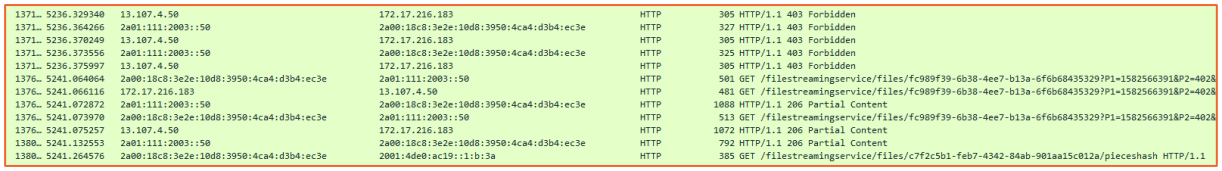
Om verkeer van een bepaald type te onderzoeken (bijvoorbeeld DHCP, ARP, HTTP of alleen verkeer van TCP poort 22) dan kan dit door onderstaande filters toe te passen:

filter:
dhcp

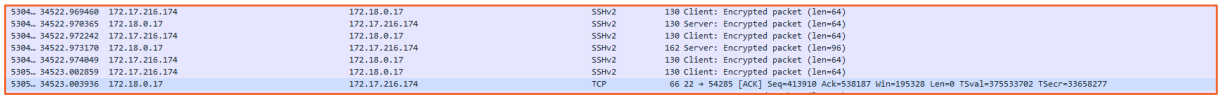
filter:
arp



filter:
http

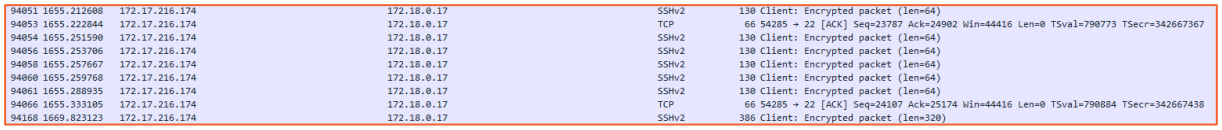


filter:
tcp.port eq 22



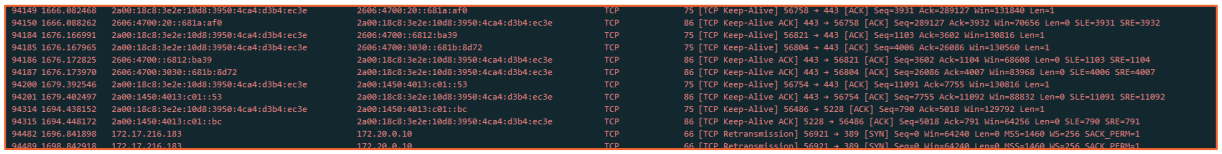
Het is ook mogelijk om filters te combineren, om bijvoorbeeld in te zoomen op TCP verkeer van poort 22 dat afkomstig is van een specifiek IP adres.

filter:
tcp.port eq 22 && ip.src == 172.17.216.174

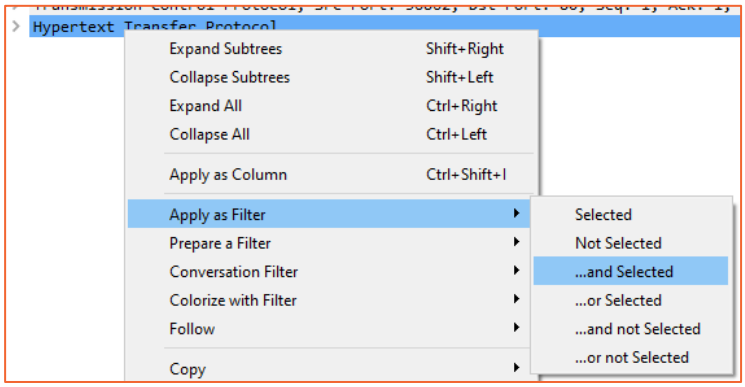


Een andere optie is bijvoorbeeld het zoeken naar pakketten met informatie of waarschuwingen zoals re transmissies, dubbele ACK’s of out-of-orders.

filter:
tcp.analysis.flags



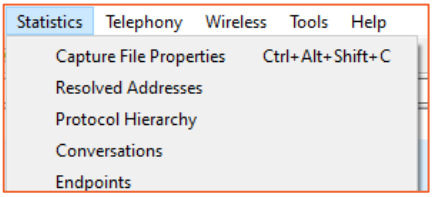
3.2 Apply as filter functie



Een andere manier om een filter toe te voegen of uit te breiden is door middel van een optie uit de "apply as filter" functie toe te passen op een selectie uit een pakket.
In bovenstaande afbeelding is zichtbaar hoe uit een pakket het HTTP protocol aan het bestaande filter wordt toegevoegd.

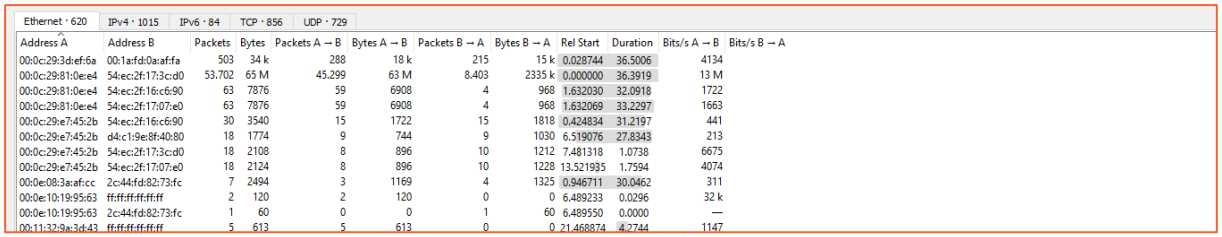
3.3 Conversation

Wireshark biedt ook de mogelijkheid om specifiek in te zoomen op conversations of anders gezegd het verkeer tussen twee specifieke hosts.

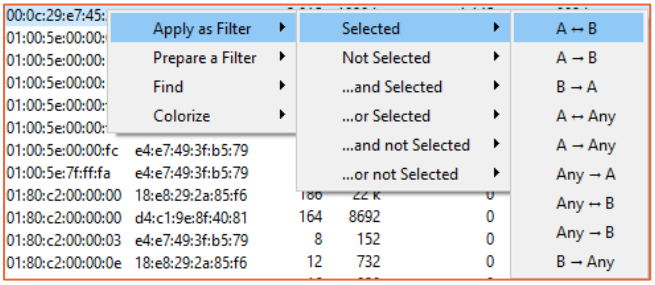


Via het menu op de taakbalk kan worden gekozen voor de optie **Statistics -> Conversation**. Er wordt vervolgens een scherm weergegeven die statistieken laat zien van alle conversations uit de packet capture.

Onderstaand screenshot toont een voorbeeld van deze statistieken. Op basis hiervan kan snel inzichtelijk worden gemaakt welke conversatie veel data verstuurd.



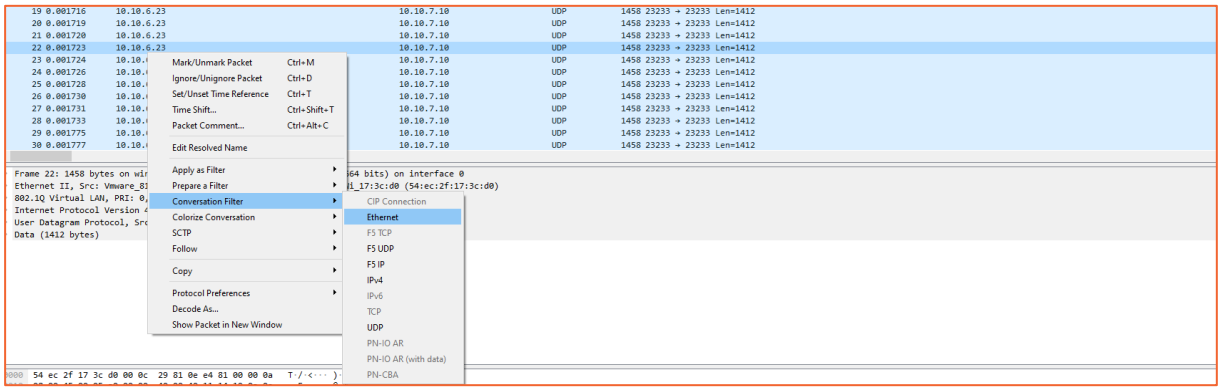
Op een specifieke conversatie inzoomen kan op twee manieren:



In vorig screenshot kan, door met de rechtermuisknop op een conversatie te klikken, deze als filter worden toegepast. Hierbij kan worden geselecteerd welk verkeer precies zichtbaar gemaakt wordt; bijvoorbeeld al het verkeer tussen A en B of alleen verkeer van A naar B. Dit resulteert in onderstaand filter:

filter
eth.addr==00:0c:29:e7:45:2b && eth.addr==e4:e7:49:3f:b5:79

Een andere manier is het selecteren van een pakketje in het hoofdscherm om dan vervolgens op via de rechtermuisknop op conversation te klikken zoals wordt weergegeven in onderstaande afbeelding.

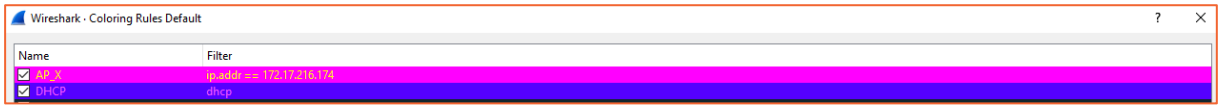


Dit resulteert weer in onderstaand filter die ook het verkeer tussen beide hosts laat zien.

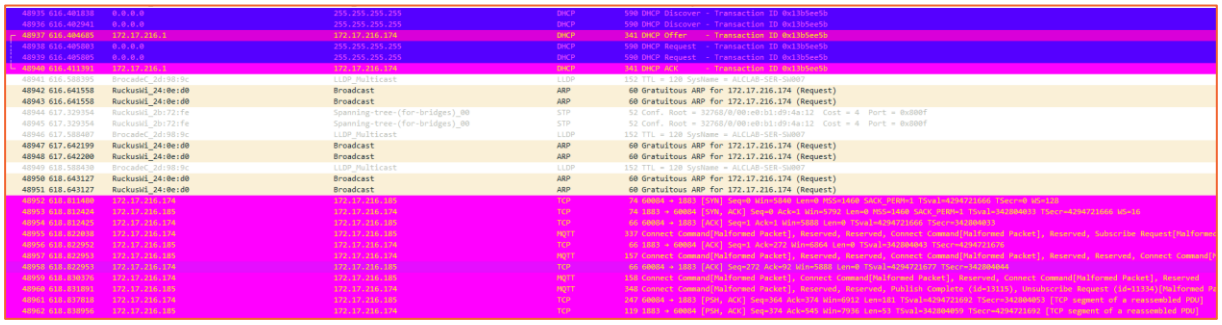
filter
eth.addr eq 00:0c:29:81:0e:e4 and eth.addr eq 54:ec:2f:17:3c:d0

3.4 Coloring rules

Om in de wireshark output snel verkeer van een bepaald type te kunnen zien kan worden gewerkt met coloring rules. Deze coloring rules kunnen worden ingesteld op basis van display filters.
In onderstaand voorbeeld heeft alle verkeer van en naar IP adres 172.17.216.174 een magenta kleur gekregen en alle DHCP verkeer blauw.



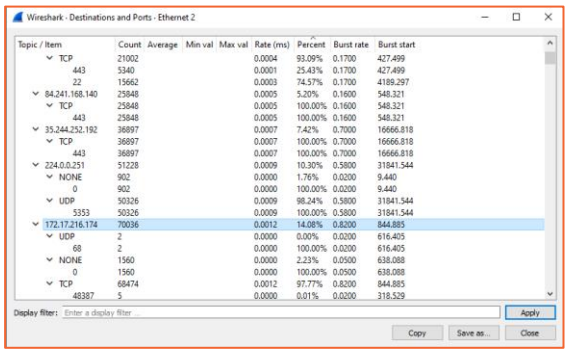
Effect:



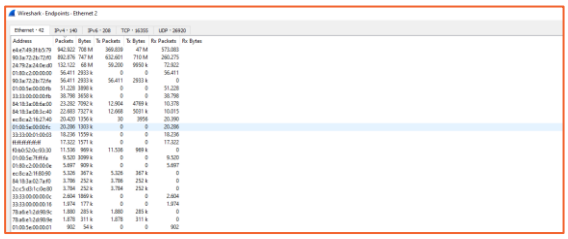
3.5 Wireshark tools

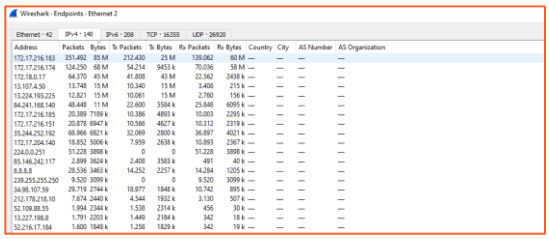
In wireshark zitten ook nog een aantal analyse tools ingebouwd die inzicht kunnen geven in de packet capture en het verkeer.

Er is bijvoorbeeld een tool om statistieken weer te geven van poorten en type verkeer gesorteerd op IP-adres.



Er is een tool die statistieken kan genereren op basis van ethernet of IP-adres, zodat je kan zien welke device welke hoeveelheid verkeer genereerd.





Er is een IO grafiek die verkeer visueel kan weergeven, ook bijvoorbeeld op basis van display filters. Hiermee zou je bijvoorbeeld in kaart kunnen brengen of een apparaat over tijd ineens veel meer of juist veel minder verkeer van een bepaald type genereerd.