GESTIONE DI RETI

RELAZIONE

ESERCIZIO 1: misura banda

GRUPPO 4

ALBERTO MARTINO EDOARDO COLI

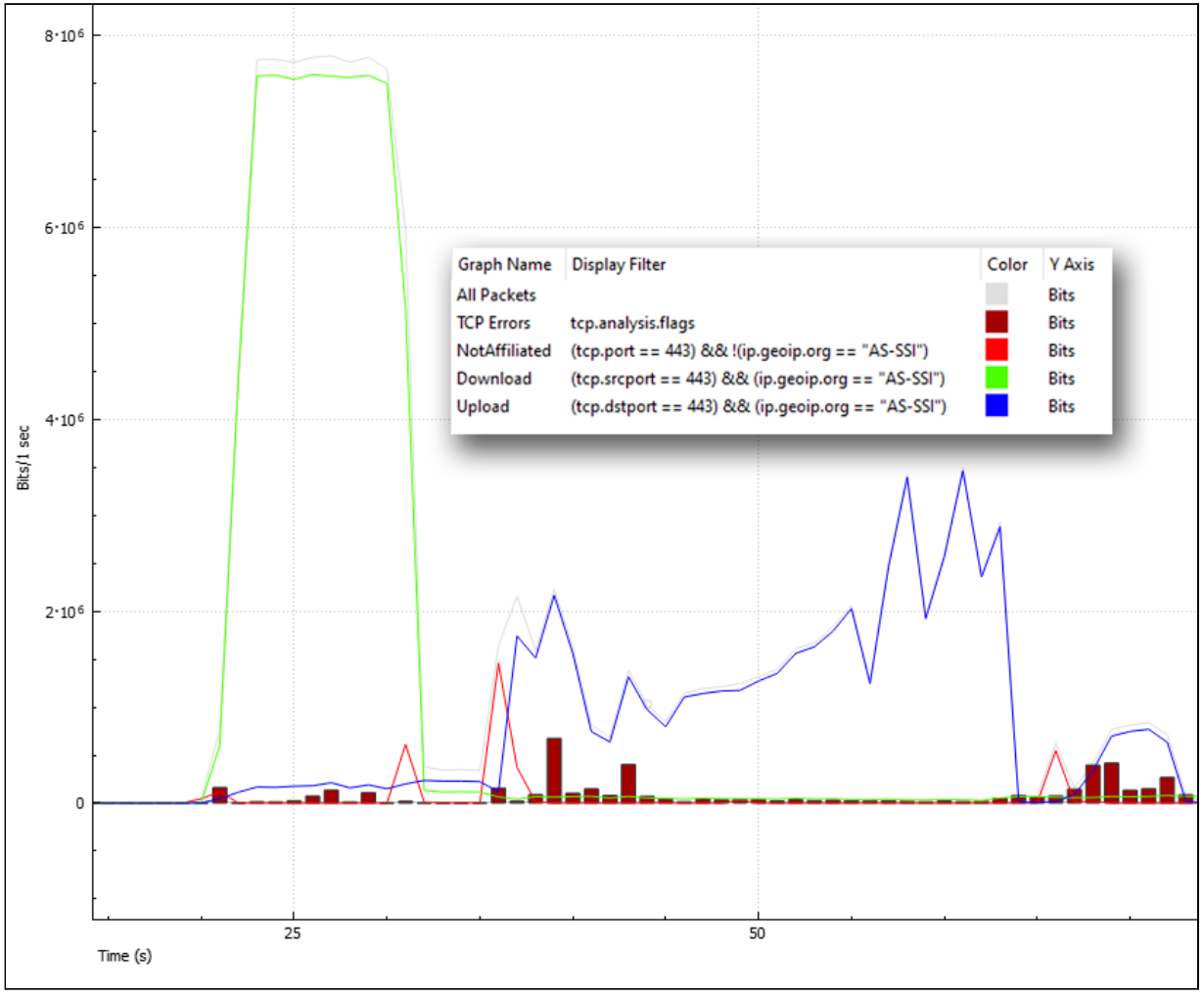
Indice

RISULTATI IN BREVE

Dopo aver catturato il traffico correlato alla misurazione di banda tramite **fast.com** abbiamo notato che:

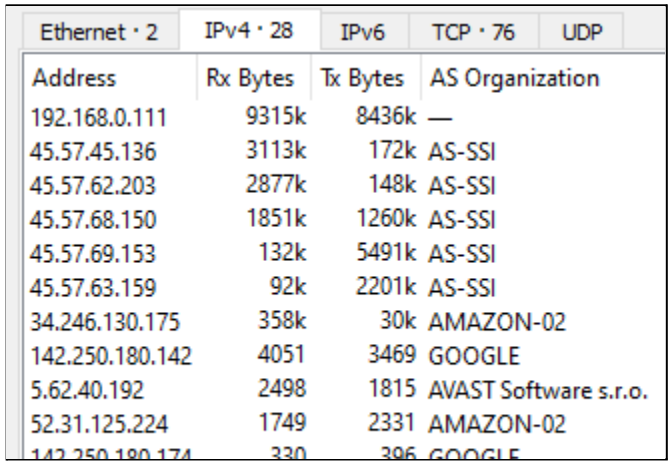
- Tale misurazione è risultata **sempre minore** (**7-12%** download, **7-42%** upload) rispetto alla banda misurata con Wireshark nonostante la percentuale di dati non misurabile (overhead pacchetti) fosse intorno allo 0.4%

- La misurazione è avvenuta utilizzando connessioni **TCP** con host multipli su **porta 443** potenzialmente associabili all'organizzazione (geoip.org) AS-SSI e con indirizzi nel range 45.0.0.0/8



IL PROCEDIMENTO

FILTRO DI CATTURA



Address	Rx Bytes	Tx Bytes	AS Organization
192.168.0.111	9315k	8436k	—
45.57.45.136	3113k	172k	AS-SSI
45.57.62.203	2877k	148k	AS-SSI
45.57.68.150	1851k	1260k	AS-SSI
45.57.69.153	132k	5491k	AS-SSI
45.57.63.159	92k	2201k	AS-SSI
34.246.130.175	358k	30k	AMAZON-02
142.250.180.142	4051	3469	GOOGLE
5.62.40.192	2498	1815	AVAST Software s.r.o.
52.31.125.224	1749	2331	AMAZON-02

Prima di tutto abbiamo cercato **quale potesse essere un filtro adeguato per la cattura** lanciando una prima cattura non filtrata.

Osservando le statistiche abbiamo identificato alcuni **host potenzialmente coinvolti nel traffico** (in particolare valutando la quantità di bit inviati/ricevuti rispetto alla media).

Osservando le statistiche di endpoints, abbiamo quindi cercato delle **caratteristiche in comune** notando che:

- geoip: l'organizzazione associata era la stessa (AS-SSI)
- ip range: tutti gli ip mittente erano nell'intervallo 45.0.0.0/8
- porta: tutti i pacchetti costituenti il flusso principale viaggiavano su porta 443

Abbiamo deciso di **ignorare il range di IP** considerando l'ampiezza dell'intervallo (molto largo) e non avendo maggiori dettagli quantitativi e qualitativi riguardo gli host e relative/a sottoreti/e.

Abbiamo deciso di **ignorare l'organizzazione** dopo aver osservato che ignorarla influisse solo sporadicamente e marginalmente sul risultato finale.

Abbiamo deciso di **sfruttare la porta TCP** per il filtro di cattura:

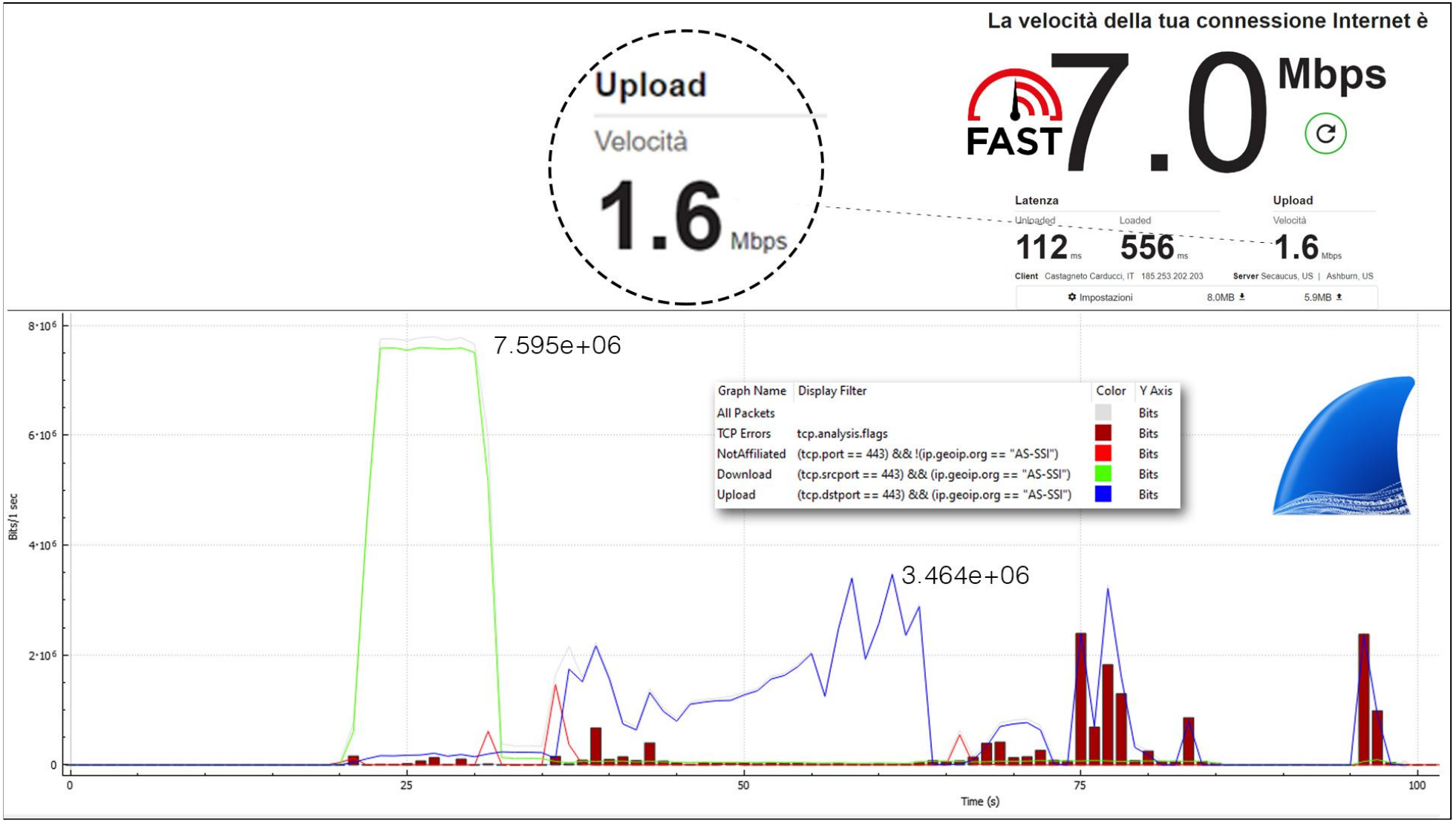
```
tcp port 443
```

riferimento: https://netflixtechblog.com/building-fast-com-4857fe0f8adb

CATTURA FILTRATA

Una volta avviata la cattura abbiamo potuto osservare i dati sul grafico che abbiamo adattato in modo che l'asse Y rappresentasse la quantità di bit così da poter confrontare con maggior facilità le due misurazioni.

Abbiamo aggiunto qualche funzione aggiuntiva per osservare alcune caratteristiche di interesse, fra le quali l'organizzazione.



ERRORI RESIDUI

Nel pcap analizzato sono stati riscontrati anche degli errori TCP che abbiamo ipotizzato essere relativi a ritrasmissioni relativi a pacchetti in upload andati persi. Aprendo le informazioni relative agli errori vediamo che il Count ha valori più elevati riguardo ad ACK duplicati e ritrasmissioni TCP, il ché è in linea con quanto osservato nel grafico per il quale abbiamo deciso di mostrare anche l'istogramma relativo agli errori TCP. Abbiamo quindi ignorato il flusso sulla porta 443 dove vi fossero queste circostanze.

Severity	Summary	Group	Proto	Count
Note	Duplicate ACK (#1)	Sequence	TCP	2872
Warning	D-SACK Sequence	Sequence	TCP	2771
Note	This frame is a (suspected) retransmission	Sequence	TCP	1170
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	214
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	213
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	136
Chat	TCP window update	Sequence	TCP	62
Chat	Connection finish (FIN)	Sequence	TCP	41
Note	ACK to a TCP keep-alive segment	Sequence	TCP	31
Note	TCP keep-alive segment	Sequence	TCP	31
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	22
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	22
Warning	Connection reset (RST)	Sequence	TCP	21
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	18
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	8
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	6
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	3
Warning	TCP Zero Window segment	Sequence	TCP	1
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	1
Warning	Ignored Unknown Record	Protocol	TLS	1

No.	Time	Protocol	Destination	Length	Info
18091	76.525883	TCP	192.168.0.111	90	443 → 52021 [ACK] Seq=5460 Ack=1122
18092	76.534891	TCP	192.168.0.111	90	[TCP Dup ACK 17775#25] 443 → 52020
18093	76.538133	TCP	192.168.0.111	90	443 → 52019 [ACK] Seq=5134 Ack=1272
18094	76.538146	TCP	192.168.0.111	90	443 → 52021 [ACK] Seq=5460 Ack=1123
18095	76.568434	TCP	192.168.0.111	90	[TCP Dup ACK 17775#26] 443 → 52020
18096	76.571637	TCP	192.168.0.111	90	443 → 52019 [ACK] Seq=5134 Ack=1276
18097	76.571651	TCP	192.168.0.111	90	443 → 52021 [ACK] Seq=5460 Ack=1125
18098	76.602337	TCP	192.168.0.111	90	443 → 52021 [ACK] Seq=5460 Ack=1126
18099	76.602372	TCP	192.168.0.111	90	[TCP Dup ACK 17775#27] 443 → 52020
18100	76.605668	TCP	192.168.0.111	82	443 → 52019 [ACK] Seq=5134 Ack=1490
18101	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18102	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18103	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18104	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18105	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18106	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [P
18107	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18108	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18109	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18110	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18111	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18112	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18113	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18114	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18115	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18116	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18117	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18118	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18119	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18120	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18121	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18122	76.605869	TCP	45.57.68.150	1414	[TCP Retransmission] 52019 → 443 [A
18123	76.605869	TCP	45.57.68.150	328	[TCP Retransmission] 52019 → 443 [F

DISCREPANZA RISULTATI

Come anticipato inizialmente, c'è una differenza significativa e inaspettata fra la misurazione di fast.com e quella ottenuta mediante Wireshark.
Lo scarto si fa **significativo** soprattutto in upload dove Wireshark misura quasi il doppio di quanto misurato da fast.com, ma anche in download non ci aspettavamo un comportamento simile immaginando che avremmo trovato, piuttosto che una sottostima, una sovrastima come visto in altri esempi a lezione.

Dopo aver valutato diverse ipotesi riguardo alle cause di tale manifestazione, riteniamo che la discrepanza fra i risultati sia dovuta a due questioni principali:

- la prima e più significativa è che, probabilmente, **la misurazione proposta da fast.com è agli effetti una media** (o un altro tipo di elaborazione della quantità di dati rispetto al tempo) invece che un upper bound come pensavamo inizialmente
- un'altra considerazione riguarda **i pacchetti ri-trasmessi dopo la misurazione**: essendo stati inviati dopo che la misurazione si è conclusa questi non solo sono stati inviati tardi ma sono stati scartati da fast.com che non ha potuto quindi tenerli in considerazione

Ci siamo chiesti anche a cosa fossero dovute queste ritrasmissioni e pensiamo che la causa sia **qualche tipo di impedimento, più o meno desiderato, che avviene (o viene effettuato) nel percorso dall'host mittente al destinatario**. Cerchiamo quindi di indagare a tale riguardo.

Per prima cosa, cerchiamo di localizzare il problema tracciando l'instradamento verso un destinatario campione durante un upload e download in contemporanea di un file di grandi dimensioni (>20GB). Questo abbiamo scelto di farlo perché al momento della misurazione il traffico di rete era occupato anche da altre connessioni (i.e. chiamata teams).

```
Traccia instradamento verso ipv4-c033-nyc005-ix.1.oca.nflxvideo.net [45.57.68.150]
su un massimo di 30 punti di passaggio:

  1     2 ms     2 ms     2 ms  192.168.0.1
  2     2 ms     2 ms     1 ms  192.168.1.254
  3     6 ms    11 ms    11 ms  172.30.8.1
  4   182 ms   192 ms   179 ms  10.255.254.129
  5   180 ms   155 ms   158 ms  10.0.2.146
  6   169 ms   174 ms   174 ms  89.202.145.109
  7   202 ms   182 ms   186 ms  et-5-3-0.cr1-mil2.ip4.gtt.net [89.149.183.121]
  8   196 ms   192 ms   188 ms  ae-17.edge1.milan1.level3.net [4.68.39.133]
  9     *        *        *     Richiesta scaduta.
 10   255 ms   276 ms   276 ms  4.7.1.138
 11   237 ms   245 ms   268 ms  ipv4-c033-nyc005-ix.1.oca.nflxvideo.net [45.57.68.150]

Traccia completata.
```

Si osserva che un primo rallentamento, notevole rispetto alla media, avviene prima di uscire dallo spazio privato.

Ipotizzando che si tratti di una regolazione fatta dall'ISP per impedire di congestionare il traffico, tracciamo l'instradamento verso 8.8.8.8 (google.com) con/senza upload e download in contemporanea di un file di grosse dimensioni.
Durante upload/download di grandi dimensioni.

```
Traccia instradamento verso dns.google [8.8.8.8]
su un massimo di 30 punti di passaggio:

  1     2 ms     6 ms     4 ms  192.168.0.1
  2     6 ms     1 ms     4 ms  192.168.1.254
  3    14 ms    20 ms    14 ms  172.30.8.1
  4   247 ms   231 ms   237 ms  10.255.254.129
  5   248 ms   239 ms   266 ms  10.0.2.146
  6   214 ms   218 ms   227 ms  89.202.145.109
  7   278 ms   278 ms   272 ms  et-5-3-0.cr1-mil2.ip4.gtt.net [89.149.183.121]
  8   264 ms   276 ms   268 ms  72.14.212.57
  9   261 ms   268 ms   254 ms  108.170.245.81
 10   234 ms   244 ms   249 ms  216.239.42.9
 11   261 ms   250 ms   263 ms  dns.google [8.8.8.8]
```

Senza upload/download di grandi dimensioni in contemporanea:

```
Traccia instradamento verso dns.google [8.8.8.8]
su un massimo di 30 punti di passaggio:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     1 ms     1 ms     1 ms  192.168.1.254
  3     9 ms    11 ms     8 ms  172.30.8.1
  4     8 ms     8 ms    10 ms  10.255.254.129
  5    10 ms     8 ms     7 ms  10.0.2.146
  6    11 ms    11 ms    11 ms  89.202.145.109
  7    21 ms    19 ms    20 ms  et-5-3-0.cr1-mil2.ip4.gtt.net [89.149.183.121]
  8    21 ms    22 ms    19 ms  72.14.212.57
  9    21 ms    19 ms    21 ms  108.170.245.81
 10    21 ms    20 ms    21 ms  216.239.42.9
 11    18 ms    20 ms    18 ms  dns.google [8.8.8.8]
```

Da questo confronto ci verrebbe da ipotizzare che l'ISP riduca in qualche modo la banda dell'host, possibilmente per evitare che questi congestioni il traffico.

Proviamo a tracciare nuovamente l'instradamento verso l'ip campione.
A questo punto notiamo come fino a Milano, a differenza di prima, non ci siano problemi.
Qui osserviamo però che vi è un altro incremento sostanziale da Milano verso il server di Netflix.

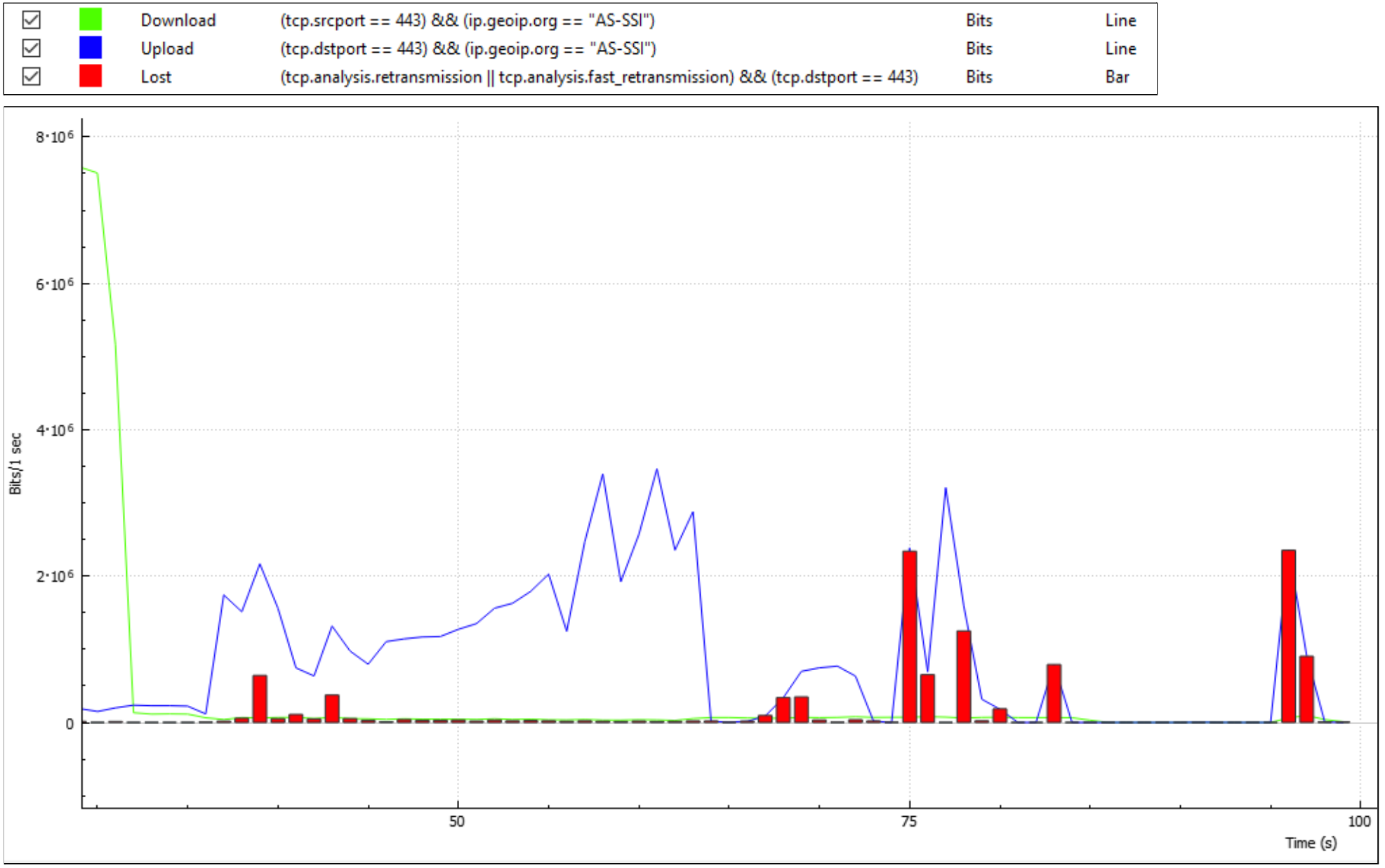
```
Traccia instradamento verso ipv4-c033-nyc005-ix.1.oca.nflxvideo.net [45.57.68.150]
su un massimo di 30 punti di passaggio:

  1     2 ms     2 ms     2 ms  192.168.0.1
  2     3 ms     3 ms     4 ms  192.168.1.254
  3     7 ms     8 ms     7 ms  172.30.8.1
  4     8 ms    10 ms     8 ms  10.255.254.129
  5     8 ms     7 ms     8 ms  10.0.2.146
  6    12 ms    11 ms    14 ms  89.202.145.109
  7    28 ms    20 ms    21 ms  et-5-3-0.cr1-mil2.ip4.gtt.net [89.149.183.121]
  8    27 ms    24 ms    19 ms  ae-17.edge1.milan1.level3.net [4.68.39.133]
  9     *        *        *     Richiesta scaduta.
 10   106 ms   109 ms   110 ms  4.7.1.138
 11   110 ms   110 ms   106 ms  ipv4-c033-nyc005-ix.1.oca.nflxvideo.net [45.57.68.150]
```

Ma non riteniamo che questo sia anomalo visto che, considerando che per raggiungere il destinatario dobbiamo raggiungere New York, la distanza geografica percorsa giustificherebbe la latenza.

In sintesi: la discrepanza dei risultati ipotizziamo sia dovuta principalmente ad una mal interpretazione dello scenario (come viene misurata la banda da fast.com) e, in modo meno incisivo ma comunque significativo, da pacchetti non ricevuti/inviati correttamente e quindi ritrasmessi (anche dopo la misurazione).
Attribuiamo come causa della perdita di pacchetti un qualche tipo di regolazione imposta dall'ISP per evitare congestioni del traffico della propria rete.

Per quanto riguarda l'impatto delle ritrasmissioni sui risultati, abbiamo già anticipato che non costituiscono un fattore determinante legato alle discrepanze ma sono comunque significativi. Per vedere con maggiore precisione questo aspetto abbiamo analizzato nuovamente il pcap visualizzando tutti i bit dei pacchetti ritrasmessi dopo la misurazione per comprendere quanti dati siano stati sicuramente ignorati da fast.com



Dal grafico si vede quanto le ritrasmissioni non siano trascurabili ma che il loro impatto (considerando ad esempio la misurazione di banda fatta per media) non sia comunque determinante principale delle discrepanze.