“Progettazione di Servizi Web e Reti di Calcolatori” (01NBEPL)
Politecnico di Torino – AA 2019/20
Prof. Antonio Lioy

Soluzioni del laboratorio n. 2

Sommario

Parametri di nslookup utili per l’esercitazione: 1
Esercizio 2.1 1
Esercizio 2.2 3
Esercizio 2.3 6
Esercizio 2.4 7
Esercizio 2.5 8
Esercizio 2.6 11
Esercizio 2.7 13
Esercizio 2.8 14
Appendice 19

Parametri di nslookup utili per l’esercitazione:

Parametro di nslookup	Tipo di query
A	Indirizzo IPv4
AAAA	Indirizzo IPv6
MX	Mail server del/i nome/i di dominio (Mail Exchanger)
NS	Name server del nome di dominio
PTR	Record “Pointer” (mostra il/i nome/i host di un indirizzo IP)
SOA	Record “Start of Authority” (indicazioni sulla gestione della zona DNS)

Esercizio 2.1

Il servizio DNS permette di mantenere la corrispondenza tra indirizzi IP e nomi attraverso interrogazioni dirette (da nome a IP) ed inverse (da IP a nome). L’architettura gerarchica e l’implementazione distribuita rendono il servizio DNS robusto e scalabile. Questa struttura influenza la risoluzione, in particolare il flusso di query e risposte, secondo quanto visto a lezione. Al fine di comprendere meglio il processo di risoluzione da nome a indirizzo IP, si eseguano in modalità manuale le query che effettuerebbe un server DNS locale per “risolvere” www.google.com.

1. Si effettui la query DNS usando il comando nslookup e specificando un root server a scelta (lista completa: http://root-servers.org/) ed il nome "www.google.com.". Quali server possono essere consultati per il "top level domain" (TLD) "com."?

Consultando la pagina web specificata è possibile trovare la lista degli indirizzi IP (versione 4 e 6) dei root nameserver.

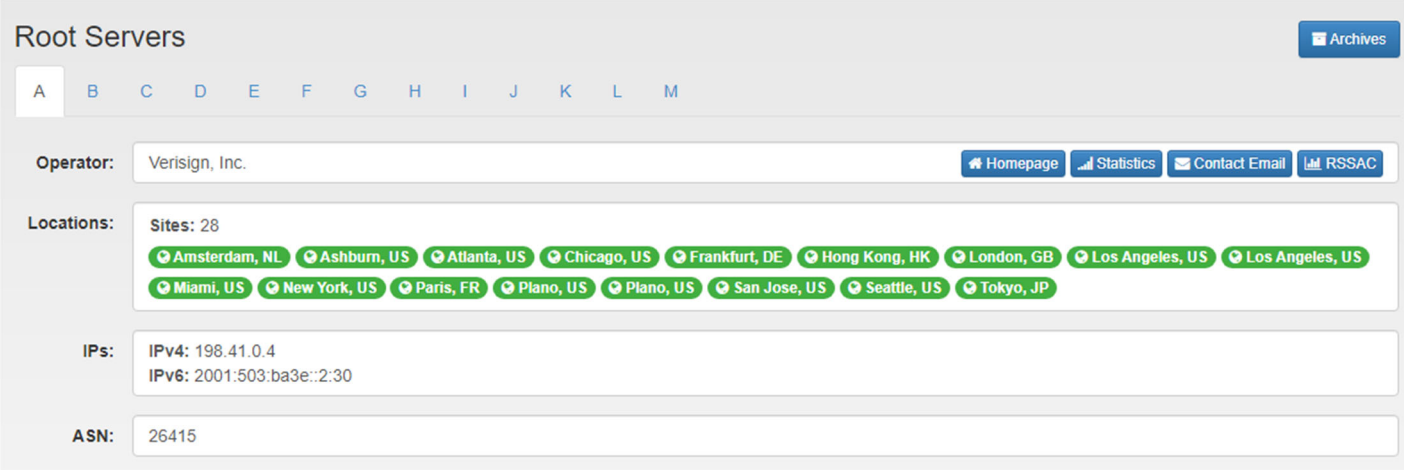


Figura 1: Lista degli indirizzi IP di alcuni root nameserver

Ad esempio scegliamo l'indirizzo "198.41.0.4" e specifichiamo che stiamo ricercando gli indirizzi IP dei server DNS responsabili del TLD .com. Il comando da impartire è:

```
nslookup -q=NS com. 198.41.0.4
```

Nota: negli esempi di comandi utilizzati viene spesso incluso anche l'indirizzo IP, ma anche comandi che includano solo il nome DNS sarebbero sufficienti.

Per ulteriori dettagli, si faccia riferimento all'Appendice.

I server da consultare saranno:

```
a.gtld-servers.net      internet address = 192.5.6.30
b.gtld-servers.net      internet address = 192.33.14.30
c.gtld-servers.net      internet address = 192.26.92.30
d.gtld-servers.net      internet address = 192.31.80.30
e.gtld-servers.net      internet address = 192.12.94.30
f.gtld-servers.net      internet address = 192.35.51.30
g.gtld-servers.net      internet address = 192.42.93.30
h.gtld-servers.net      internet address = 192.54.112.30
i.gtld-servers.net      internet address = 192.43.172.30
j.gtld-servers.net      internet address = 192.48.79.30
k.gtld-servers.net      internet address = 192.52.178.30
l.gtld-servers.net      internet address = 192.41.162.30
m.gtld-servers.net      internet address = 192.55.83.30
a.gtld-servers.net      AAAA IPv6 address = 2001:503:a83e::2:30
b.gtld-servers.net      AAAA IPv6 address = 2001:503:231d::2:30
```

Figura 2: esempio di output del comando nslookup -q=NS per il dominio .com

2. Scegliere un server responsabile della gestione del TLD "com.". Effettuare la precedente query specificando il nuovo server DNS. Compilare la lista dei server DNS disponibili:

Per identificare i nameserver responsabili del dominio google.com è necessario effettuare una nuova query specificando un nameserver a scelta tra quelli disponibili per il TLD .com.

Ad esempio scegliamo l'indirizzo "192.12.94.30" per identificare i nameserver responsabili per il dominio google.com. Il comando da impartire è

nslookup -q=NS google.com. 192.12.94.30

per ulteriori dettagli, si faccia riferimento all'Appendice..

```
C:\Users\ASUS>nslookup -q=NS google.com. 192.12.94.30
(root)  nameserver = b.root-servers.net
(root)  nameserver = c.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = e.root-servers.net
(root)  nameserver = f.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = j.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = l.root-servers.net
(root)  nameserver = m.root-servers.net
(root)  nameserver = a.root-servers.net
Server:  UnKnown
Address:  192.12.94.30

google.com      nameserver = ns2.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns4.google.com
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns2.google.com  internet address = 216.239.34.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns1.google.com  internet address = 216.239.32.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns4.google.com  internet address = 216.239.38.10
```

Figura 3: esempio di output del comando nslookup -q=NS

3. In modo simile ai punti precedenti, scegliere un server dalla lista e identificare tutti gli indirizzi IP associati a "www.google.com.":

Per identificare gli indirizzi IP versione 4 associati a www.google.com è necessario effettuare una query specificando come server da interrogare uno dei nameserver disponibili per il dominio google.com, ad esempio scegliamo "216.239.32.10" per effettuare la query.

Il comando da impartire è:

nslookup -q=NS www.google.com. 216.239.32.10

per ulteriori dettagli, si faccia riferimento all'Appendice.

```
C:\Users\ASUS>nslookup -q=NS www.google.com. 216.239.32.10
Server:  ns1.google.com
Address:  216.239.32.10

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 303291920
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

Figura 4: esempio di output della query di tipo NS per google.com

Esercizio 2.2

Usando il comando nslookup e relative opzioni

1. Identificare i nameserver del dominio "libero.it" e fornire le seguenti risposte:

a. comando ed opzioni:

Si vogliono identificare i nameserver primario e secondario per il dominio in oggetto. In modo analogo a quanto fatto precedentemente, cerchiamo gli indirizzi IP dei server DNS responsabili del TLD it.

nslookup -q=NS it. 198.41.0.4

```
C:\Users\ASUS>nslookup -q=NS it. 198.41.0.4
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  198.41.0.4

it      nameserver = a.dns.it
it      nameserver = m.dns.it
it      nameserver = r.dns.it
it      nameserver = s.dns.it
it      nameserver = dns.nic.it
it      nameserver = nameserver.cnr.it
a.dns.it        internet address = 194.0.16.215
m.dns.it        internet address = 217.29.76.4
r.dns.it        internet address = 193.206.141.46
s.dns.it        internet address = 194.146.106.30
dns.nic.it      internet address = 192.12.192.5
nameserver.cnr.it       internet address = 194.119.192.34
a.dns.it        AAAA IPv6 address = 2001:678:12:0:194:0:16:215
m.dns.it        AAAA IPv6 address = 2001:1ac0:0:200:0:a5d1:6004:2
r.dns.it        AAAA IPv6 address = 2001:760:ffff:ffff::ca
s.dns.it        AAAA IPv6 address = 2001:67c:1010:7::53
dns.nic.it      AAAA IPv6 address = 2a00:d40:1:1::5
nameserver.cnr.it       AAAA IPv6 address = 2a00:1620:c0:220:194:119:192:34
```

Figura 5: esempio di output del comando nslookup -q=NS per il dominio it.

Effettuiamo una nuova query specificando un nameserver a scelta tra quelli disponibili per il TLD .it, ad esempio 193.206.141.46.

I comandi da impartire sono:

nslookup -q=NS libero.it. 193.206.141.46

nslookup -q=SOA libero.it. 193.206.141.46 *(per stabilire il primario)*

```
C:\Users\ASUS>nslookup -q=NS libero.it. 193.206.141.46
Server:  UnKnown
Address:  193.206.141.46

libero.it       nameserver = n2.libero.it
libero.it       nameserver = n1.libero.it
n1.libero.it    internet address = 156.154.66.47
n2.libero.it    internet address = 156.154.67.47
```

Figura 6: esempio di output del comando nslookup -q=NS per libero.it

b. Name server primario: n1.libero.it

c. Name server secondari: n2.libero.it

La risposta non proviene da un server "authoritative". Bisogna specificare l'indirizzo IP del server primario trovato al punto precedente (n1.libero.it, il cui indirizzo IP è 156.154.66.47).

Il comando da impartire è:

```
nslookup -q=NS libero.it. n1.libero.it
```

oppure

```
nslookup -q=NS libero.it. n2.libero.it
```

(la risposta è authoritative anche se non arriva direttamente dal primario).

2. Identificare gli indirizzi e i nomi dei server destinati a offrire il servizio di posta elettronica per il dominio "libero.it":

a. comando e opzioni:

```
nslookup -q=MX libero.it.
```

che ci fornisce il Mail server del/i nome/i di dominio (Mail Exchanger).

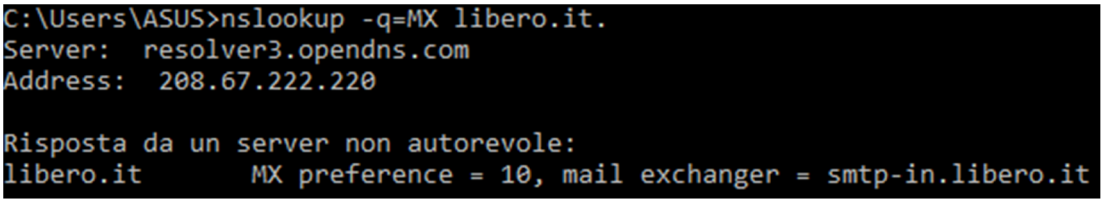


Figura 7: Esempio di output per il comando nslookup -q=MX per libero.it

b. nome e indirizzo IP del server di posta:

L'output del comando nslookup –q=MX mostra il nome del Mail Server, ma non il suo indirizzo IP. Per trovarlo è necessario effettuare una nuova query di tipo A, attraverso la quale potremo conoscere l'IP pubblico che viene usato per consegnare le mail al mail server di destinazione.

```
nslookup -q=A smtp-in.libero.it
Server:  smtp-in.libero.it
Address:  213.209.1.129
```

3. La risposta del punto precedente proviene da un server authoritative? Se così non fosse, come deve essere modificato il comando per ricevere una risposta da un server authoritative?

Come è possibile vedere dall'output, la risposta non proviene da un server "authoritative". Bisogna specificare l'indirizzo IP del server primario trovato al punto precedente (n1.libero.it, il cui indirizzo IP è 156.154.66.47).

Il comando da impartire è:

```
nslookup -q=MX libero.it. 156.154.66.47
```

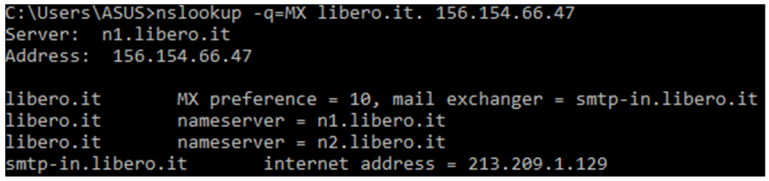


Figura 8: esempio di output del comando nslookup -q=MX verso il server primario

4.Come è possibile determinare gli alias per l'host "www.libero.it"?

a. comando e opzioni:

```
nslookup -q=CNAME www.libero.it. 156.154.66.47
```

```
C:\Users\ASUS>nslookup -q=CNAME www.libero.it. 156.154.66.47
Server:  n1.libero.it
Address:  156.154.66.47

www.libero.it   canonical name = d31d9gezsyt1z8.cloudfront.net
libero.it       nameserver = n1.libero.it
libero.it       nameserver = n2.libero.it
```

Figura 9: esempio di output per il comando nslookup -q=CNAME

b. alias:

www.libero.it è l'alias di d31d9gezsyt1z8.cloudfront.net.

Esercizio 2.3

Usando il comando nslookup e relative opzioni, identificare per l'indirizzo IP "130.192.1.34" gli FQDN corrispondenti.

Per identificare il nome associato all'indirizzo 130.192.1.34 possiamo effettuare una query richiedendo il record PTR che è un puntatore ad un nome canonico utilizzato per la risoluzione DNS inversa.

```
nslookup -q=PTR 130.192.1.34
```

L'opzione –q=PTR richiede il record PTR descritto sopra.

Un possibile output ottenuto dal comando è:

```
C:\Users\ASUS>nslookup -q=PTR 130.192.1.34
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
34.1.192.130.in-addr.arpa       name = taurus.polito.it
```

Figura 10: esempio di output per il comando nslookup -q=PTR

1. Nome DNS corrispondente: taurus.polito.it
2. Comando e opzioni utilizzate: nslookup –q=PTR 130.192.182.33
3. Eventuali aliasi associati:

per determinare gli alias eseguiamo gli stessi comandi degli esercizi precedenti:

```
nslookup -q=A it. 198.41.0.4
```

```
nslookup -q=NS taurus.polito.it 193.206.141.46
```

```
C:\Users\ASUS>nslookup -q=NS taurus.polito.it 193.206.141.46
Server:  UnKnown
Address:  193.206.141.46

DNS request timed out.
    timeout was 2 seconds.
polito.it       nameserver = ns1.garr.net
polito.it       nameserver = ns3.polito.it
polito.it       nameserver = leonardo.polito.it
polito.it       nameserver = giove.polito.it
ns3.polito.it   internet address = 130.192.4.30
giove.polito.it internet address = 130.192.3.24
leonardo.polito.it      internet address = 130.192.3.21
```

Figura 11: esempio di output per il comando nslookup -q=NS

Vediamo dall'output che non ci sono alias associati.

Trovare poi l'indirizzo IP associato al nome "security.polito.it": quali considerazioni si possono fare dopo questa operazione?

Il comando da impartire è:

```
nslookup -q=A security.polito.it
```

```
C:\Users\ASUS>nslookup -q=A security.polito.it
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
Nome:    taurus.polito.it
Address:  130.192.1.34
Aliases:  security.polito.it
```

Figura 12: esempio di output per il comando nslookup -q=A

Inserendo il comando

```
nslookup -q=CNAME security.polito.it
```

```
C:\Users\ASUS>nslookup -q=CNAME security.polito.it
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
security.polito.it      canonical name = taurus.polito.it
```

Figura 13: esempio di output per il comando nslookup -q=CNAME

security.polito.it è l'alias di taurus.polito.it, ma non il contrario. Questo significa che non è possibile identificare la relazione tra i due a partire da taurus.polito.it.

Esercizio 2.4

Alcuni server applicativi fanno una doppia query al DNS per verificare l'identità dei client prima di accettarne le richieste: sono i cosiddetti server paranoici (in inglese: paranoid server). Se le risposte di lookup diretto e inverso sono coerenti, allora rispondono alla richiesta.

Seguendo questo principio, elencare i passaggi ed i comandi necessari per eseguire manualmente con il comando nslookup i passi effettuati da un server paranoico per verificare la corrispondenza biunivoca nome-indirizzo per i nodi con indirizzi 130.192.181.193 (corrispondente a webfront-01.polito.it) e 193.42.161.169 (corrispondente a www.mondadori.it). Quali differenze notate?

Per identificare il nome associate all'indirizzo 130.181.193 possiamo effettuare una query richiedendo il record PTR che è un puntatore ad un nome canonico utilizzato per la risoluzione DNS inversa.

```
nslookup -q=PTR 130.192.181.193
```

Un possibile output ottenuto dal comando è:

```
C:\Users\ASUS>nslookup -q=PTR 130.192.181.193
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
193.181.192.130.in-addr.arpa    name = webfront-01.polito.it
```

Figura 14: esempio di output per il comando nslookup -q=PTR

Possiamo dunque stabilire che il nome canonico associato all'indirizzo IP 130.192.181.193 è webfront-01.polito.it.

La risoluzione inversa è ottenuta interrogando il server DNS della rete locale in quanto non è stato specificato nessun server esterno. Inoltre, la risposta proviene da un server "non-authoritative".

Successivamente per verificare che l'indirizzo IP associato a webfront-01-polito.it sia 130.192.181.193 dovremmo eseguire la seguente query attraverso il comando:

```
nslookup -q=A webfront-01.polito.it
```

L'opzione –q=A restituisce la lista degli indirizzi IP versione 4 associati ad un nome, come spiegato in precedenza.

L'output ottenuto dal comando è:

```
C:\Users\ASUS>nslookup -q=A webfront-01.polito.it
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
Nome:    webfront-01.polito.it
Address:  130.192.181.193
```

Figura 15: esempio di output per il comando nslookup -q=A

Da cui l'indirizzo IP versione 4 associato al nome web farm.polito.it è 130.192.181.193.

E' stata quindi verificata la corrispondenza biunivoca nome-indirizzo.

Si osservi che la risoluzione è ottenuta interrogando il server DNS della rete locale in quanto non è stato specificato nessun server esterno. Inoltre, la risposta proviene da un server "non-authoritative". Per esser sicuri che la cache DNS non sia diventata obsoleta, si potrebbero ripetere i passi di cui sopra, avendo cura di interrogare un server "authoritative".

Per il secondo indirizzo proposto, 193.42.161.169, si può ripetere la stessa procedura. In questo caso però la seconda query (con opzione –q=A) non andrebbe a buon fine, quindi un server paranoico non fornirebbe a questo host una risposta.

```
C:\Users\ASUS>nslookup -q=A mondadori.it
Server:  resolver3.opendns.com
Address:  208.67.222.220

Risposta da un server non autorevole:
Nome:    mondadori.it
Address:  193.42.160.4
```

Figura 16: esempio di output per il comando nslookup -q=A

Esercizio 2.5

Si vogliono analizzare i pacchetti DNS scambiati durante la risoluzione del nome www.google.com.

A tal fine si segua la seguente procedura e si risponda alle domande proposte.

Aprire wireshark, predisporlo alla cattura dei pacchetti DNS (specificando l'interfaccia di rete) ed avviare la cattura dei pacchetti.

Attraverso l'applicativo nslookup eseguire la query richiesta.

Eseguiamo le stesse query dell'esercizio 2.1:

```
nslookup -q=A com. 198.41.0.4

nslookup -q=NS google.com. 192.12.94.30

nslookup -q=A www.google.com. 216.239.32.10
```

un esempio di cattura di wireshark è il seguente:

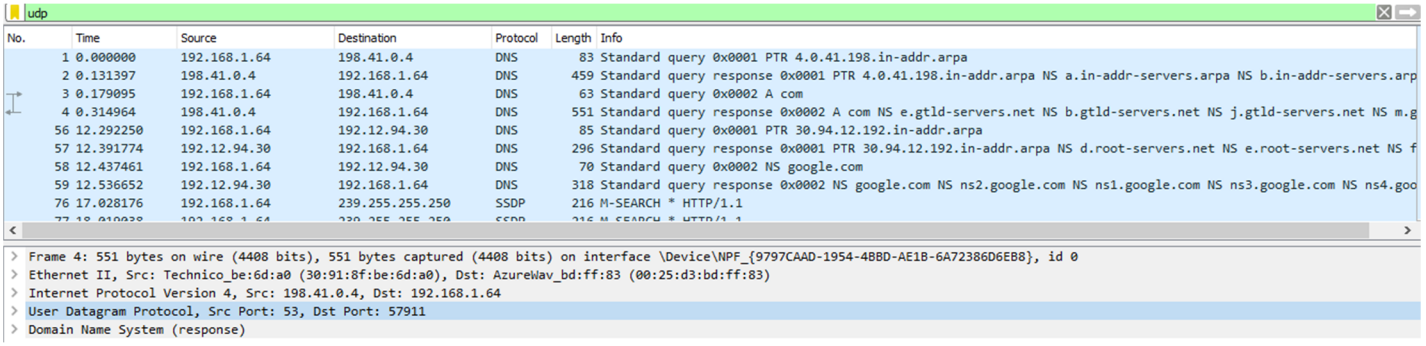


Figura 17: esempio di cattura wireshark a seguito di risoluzione del nome

1. Quali protocolli della pila TCP/IP, partendo dal livello "data-link", sono stati impiegati?

Come detto precedentemente, per ogni pacchetto è possibile visualizzare i vari protocolli utilizzati nello stack ISO/OSI , semplicemente guardando nella seconda suddivisione della finestra principale. Pertanto come possiamo vedere, i protocolli in questo caso sono:

- Ethernet

- IPv4

- UDP

- DNS

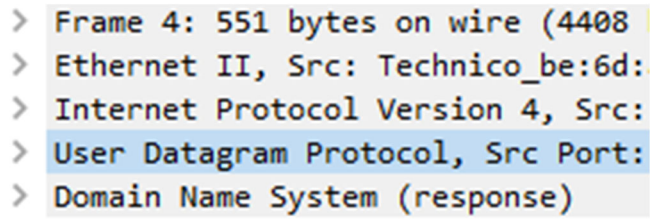
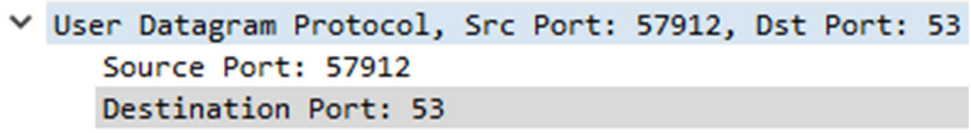


Figura 18: visualizzazione di wireshark dei protocolli utilizzati

2. Quali "porte" del protocollo di trasporto sono state usate? Il loro identificativo nelle varie prove è fisso o variabile? Il loro identificativo è, in generale, necessariamente fisso/variabile (cioè, quanto riscontrato in queste prove è una regola sempre vera)?

Attraverso la colonna info, con la dicitura query e query response è possibile dedurre chi sia il client e chi il server nelle colonne Source e Destination. Una volta identificati, analizzando ad esempio i vari messaggi di query, è possibile notare come la porta usata dal DNS Server sia sempre uguale (numero 53). Per quanto riguarda la porta del client invece si nota come cambi ad ogni richiesta DNS ed è sempre superiore a 1024. Questo avviene perché il DNS server deve sempre essere in ascolto di richieste DNS, per cui rimane in attesa sulla porta nota (porta privilegiata) a 53, lato client invece è sufficiente utilizzare come porta mittente una qualsiasi porta utente (da 1024 a 65535) che sia libera, dunque ne viene assegnata una in automatico dal sistema operativo. Infatti non è necessario che il DNS Server conosca a priori l'indirizzo e porta del Client, semplicemente accetta tutte le richieste, purchè siano destinate alla porta 53.



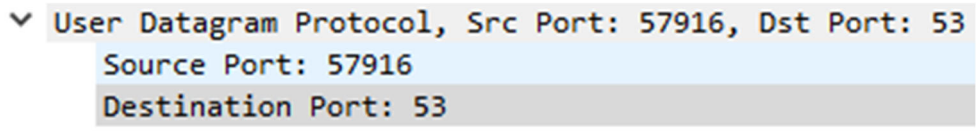


Figura 19: esempi di porte sorgente e destinazione

3. E' possibile identificare la query richiesta al server DNS? In caso affermativo compilare i seguenti campi:

E' possibile identificare il pacchetto come query DNS dalla colonna Info,

mentre aprendo la riga dello stack protocollare del protocollo DNS ed esaminando

il contenuto della tendina "Queries" sono visualizzabili i campi richiesti.

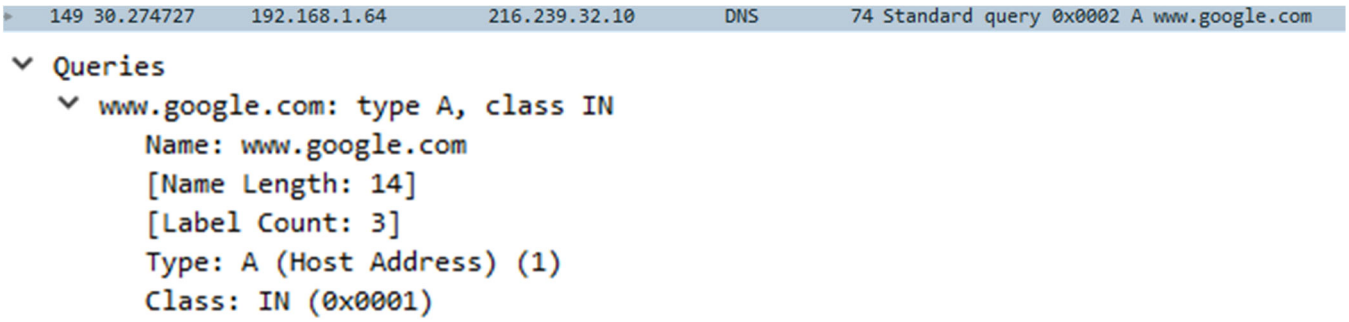


Figura 20: campi visualizzabili nella colonna "Queries"

a) Name: www.google.com

b) Type: A

c) Class: IN

Nello specifico il valore di tipo "A" sta ad indicare la richiesta di un indirizzo IPv4, mentre il valore di classe "IN" sta a indicare un dominio Internet.

4. E' possibile identificare la risposta del DNS? In caso affermativo compilare i seguenti campi per un indirizzo IP a scelta tra quelli presenti della risposta:

E' possibile identificare il pacchetto come "query response" dalla colonna info, mentre aprendo la riga dello stack protocollare del protocollo DNS ed esaminando il contenuto della tendina "Answers" sono visualizzabili i campi richiesti.

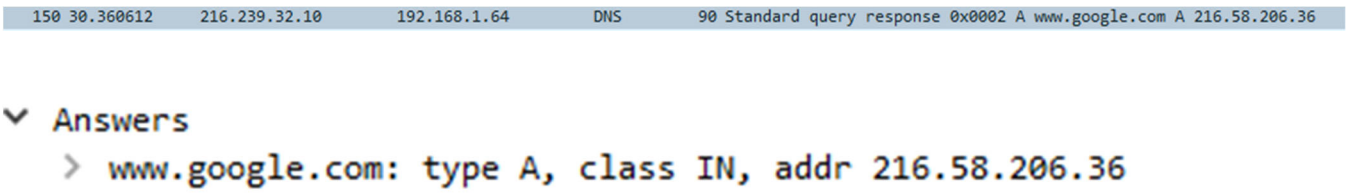


Figura 21: contenuto della tendina "Answers"

a) Name: www.google.com

b) Type: A

c) Class: IN

d) Addr: 216.58.206.36

5. Per identificare più precisamente il traffico DNS è possibile definire un filtro per la visualizzazione?

Per visualizzare il traffico DNS è sufficiente scrivere "dns" come filtro di visualizzazione, o alternativamente "udp.port==53" poiché abbiamo visto che si tratta della porta standard dei Server DNS. Se volessimo invece

impostare un filtro di intercettazione per i messaggi DNS, l'unico modo è scrivere "udp port 53" nelle opzioni di interfaccia prima di cominciare la cattura.

Esercizio 2.6

Si vuole analizzare il throughput TCP durante il download di file con diverse dimensioni.

Usando wget, scaricare i file proposti (URL http://security.polito.it/~lioy/01nbe/lab2/ seguita dal nome del file) e rispondere alle domande.

1. Eseguire il download del file 'test1k.dat' e rilevare i seguenti dati:

comando

wget http://security.polito.it/~lioy/01nbe/lab2/test1k.dat

```
C:\Users\ASUS>wget http://security.polito.it/~lioy/01nbe/lab2/test1k.dat
URL transformed to HTTPS due to an HSTS policy
--2020-03-25 19:02:34--  https://security.polito.it/~lioy/01nbe/lab2/test1k.dat
Resolving security.polito.it (security.polito.it)... 130.192.1.34
Connecting to security.polito.it (security.polito.it)|130.192.1.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1024 (1,0K)
Saving to: 'test1k.dat.5'

test1k.dat.5                100%[=================================================>]   1,00K  --.-KB/s    in 0,001s

2020-03-25 19:02:34 (1,30 MB/s) - 'test1k.dat.5' saved [1024/1024]
```

Figura 22: esempio di download tramite wget del file 'test1k.dat'

Al fine di visualizzare i byte trasferiti, il tempo richiesti per il download e il throghoput medio è sufficiente osservare i valori restituiti nel terminale usando il comando wget. E' da notare che in questo caso, scaricando il file da 1 kB, il tempo medio non viene calcolato, per via del fatto che il tempo trascorso per lo scaricamento del file è inferiore a 1s, cosa che non avviene per i file di dimensioni più grandi come quello da 10 MB.

a. byte trasferiti: 1024

b. tempo richiesto per il download: 0,001 s

c. throughput medio: --,- KB/s

2. Eseguire il download del file 'test10k.dat' e rilevare i seguenti dati:

```
C:\Users\ASUS>wget http://security.polito.it/~lioy/01nbe/lab2/test10k.dat
URL transformed to HTTPS due to an HSTS policy
--2020-03-25 19:06:19--  https://security.polito.it/~lioy/01nbe/lab2/test10k.dat
Resolving security.polito.it (security.polito.it)... 130.192.1.34
Connecting to security.polito.it (security.polito.it)|130.192.1.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K)
Saving to: 'test10k.dat'

test10k.dat                 100%[=================================================>]  10,00K  --.-KB/s    in 0,01s

2020-03-25 19:06:19 (688 KB/s) - 'test10k.dat' saved [10240/10240]
```

Figura 23: esempio di download tramite wget del file 'test10k.dat'

a. byte trasferiti: 10240

b. tempo richiesto per il download: 0.01 s

c. throughput medio: _.- kB/s

3. Eseguire il download del file 'test100k.dat' e rilevare i seguenti dati:

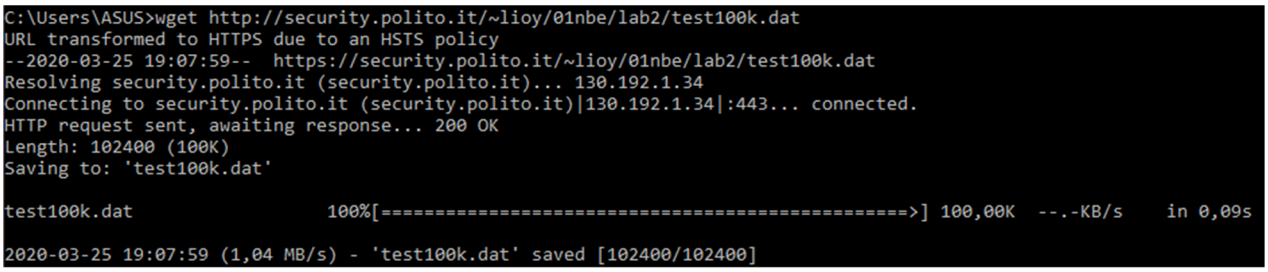


Figura 24: esempio di download tramite wget del file 'test100k.dat'

a. byte trasferiti: 102400

b. tempo richiesto per il download: 0.09 s

c. throughput medio: _.- kB/s

4. Eseguire il download del file 'test1m.dat' e rilevare i seguenti dati:

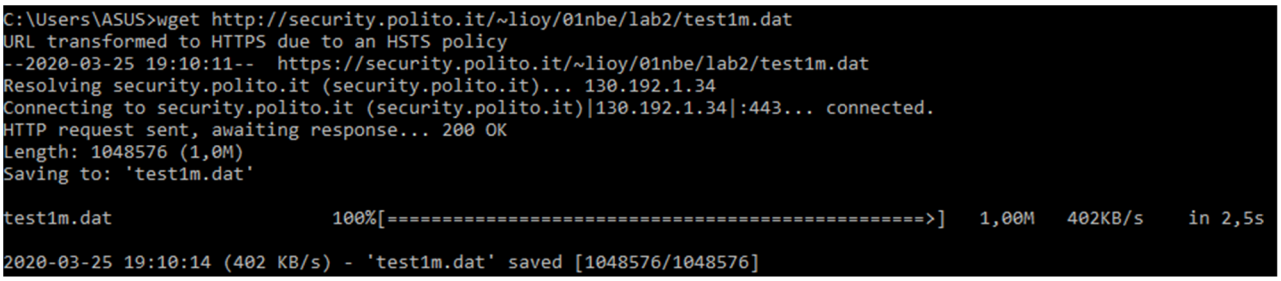


Figura 25: esempio di download tramite wget del file 'test1m.dat'

a. byte trasferiti: 1048576

b. tempo richiesto per il download: 2,5 s

c. throughput medio: 402 kB/s

5. Eseguire il download del file 'test10m.dat' e rilevare i seguenti dati:

Figura 26: esempio di download tramite wget del file 'test10m.dat'

a. byte trasferiti: 10485760

b. tempo richiesto per il download: 5,7 s

c. throughput medio: 1,60 MB/s

6. Il throughput medio varia all'aumentare delle dimensioni del file? In caso affermativo spiegare per quale ragione.

Dai 100jB in poi possiamo riuscire a valutare l'andamento del throughput medio. Vediamo che il throughput in questo esempio aumenta, ma potrebbe verificarsi anche il contrario. Questo potrebbe succedere perché la finestra di trasmissione, tipica del TCP, è in grado di aumentare di dimensione solo fino a un certo valore massimo, in base all'algoritmo utilizzato (ad esempio lo Slow Start). Altra motivazione possibile del calo del throughput potrebbe anche essere un effettivo stato di congestione della rete; in tal caso il client, che rileva questo stato, decide di decrementare la dimensione della finestra di trasmissione per tentare di risolvere il problema.

NOTA

Può capitare che la rete abbia fluttuazioni notevoli (le fluttuazioni si possono verificare effettuando la stessa prova più volte), che possono causare variazioni percentuali notevoli nei tempi di trasferimento e throughput, evidenti soprattutto in caso di trasferimenti di piccole dimensioni. In alcuni casi si può osservare, pur ripetendo l'esperimento a soli pochi secondi di distanza, una variazione di throughput anche di un ordine di grandezza su trasferimenti di qualche secondo.

Con una rete così "ballerina" è difficile cogliere la variazione al crescere della dimensione dei file, in quanto la fluttuazione sulla rete risulta maggiore del risparmio di overhead dovuto al trasferimento di dati di dimensioni maggiori in un'unica sessione. E' quindi consigliabile effettuare ripetutamente le prove (ad esempio 10 volte, ma quale sia un valore statisticamente significativo di campioni dipende anche dalla varianza della rete) ed effettuare una media per avere dati più significativi.

Esercizio 2.7

Si vuole analizzare (mediante l'utilizzo di un grafico) l'andamento della TCP window durante il download di risorse con dimensioni diverse.

Considerando gli stessi file proposti nell'esercizio precedente, si segua la procedura proposta qui sotto per ciascun file:

1. *usando gli applicativi wget e wireshark, si proceda alla cattura del traffico TCP relativo al download di un file a scelta;*
2. *usando gli applicativi wget e wireshark, si proceda alla cattura del traffico TCP relativo al download di un file a scelta;*
3. *salvare il traffico catturato in un file esterno;*
4. *personalizzare la finestra di visualizzazione aggiungendo una colonna separata che contenga il valore della TCP window;*

Prima di esportare il file CSV selezionare, attraverso il filtro di selezione, i soli pacchetti inviati dal client al server, questo perché la dimensione della finestra TCP lato server è tipicamente fissa, mentre lato client può aumentare e diminuire a seconda del traffico che il client è in grado di ricevere di volta in volta. Per fare questo dunque è sufficiente scrivere il comando "ip.src==<ip interfaccia pc", come vediamo in figura. Come valori della finestra TCP consideriamo i soli valori del trasferimento, ossia dopo HTTP GET..

1. Per ciascuna risorsa qual è la dimensione minima e massima della TCP window?

a. dimensione minima: 29200

b. dimensione massima: 30336

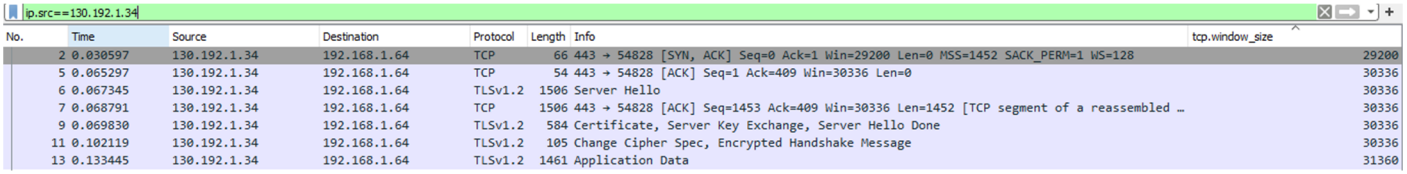


Figura 27: filtro di selezione da inserire

2.Spiegare il diverso andamento della TCP window per risorse con dimensioni diverse.

Definendo i grafici per ogni dimensione del file si ottengono i risultati delle figure. Il caso del file di 1 KB ovviamente non è considerato, poiché viene trasmesso un solo pacchetto. Negli altri casi la finestra viene decrementata ogni qualvolta vengano persi dei pacchetti, ciò determina uno stato di congestione della rete. Nel caso del file da 10 KB, la dimensione della finestra rimane costante perché il trasferimento è talmente breve che la probabilità di perdita dei pacchetti è quasi nulla. Nei trasferimenti di dimensione più grande (e quindi più duraturi) invece tale probabilità aumenta e vi si aggiungono i problemi di condivisione dinamica della banda.

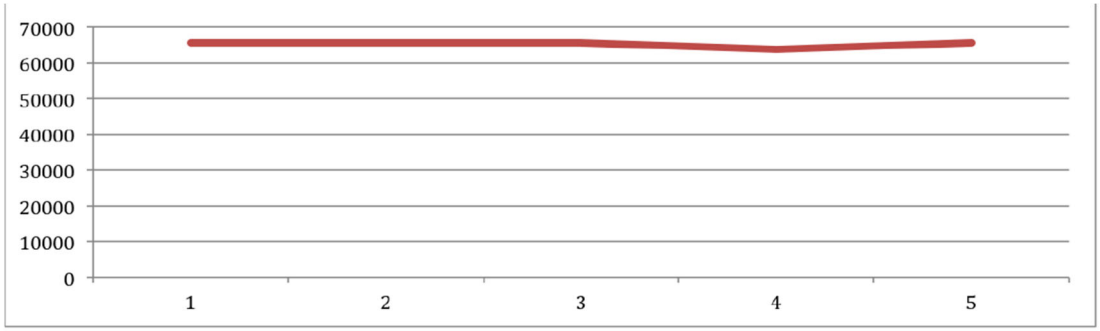


Figura 28: Grafico (numero di pacchetto - dimensione della finestra TCP) dello scaricamento del file 10 KB

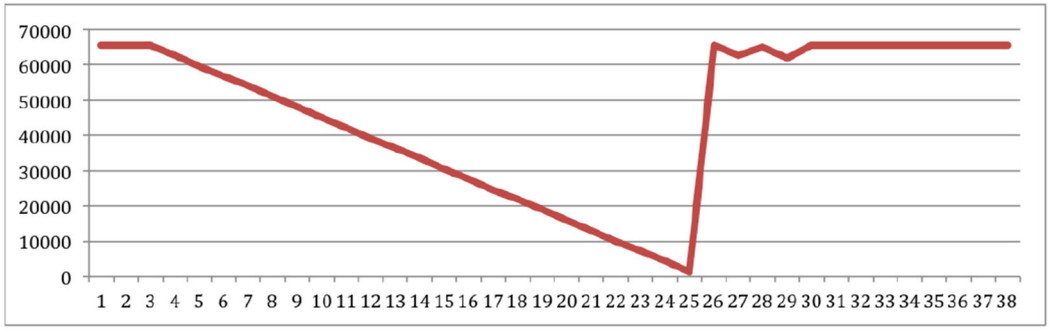


Figura 29: Grafico (numero di pacchetto - dimensione della finestra TCP) dello scaricamento del file 100 KB

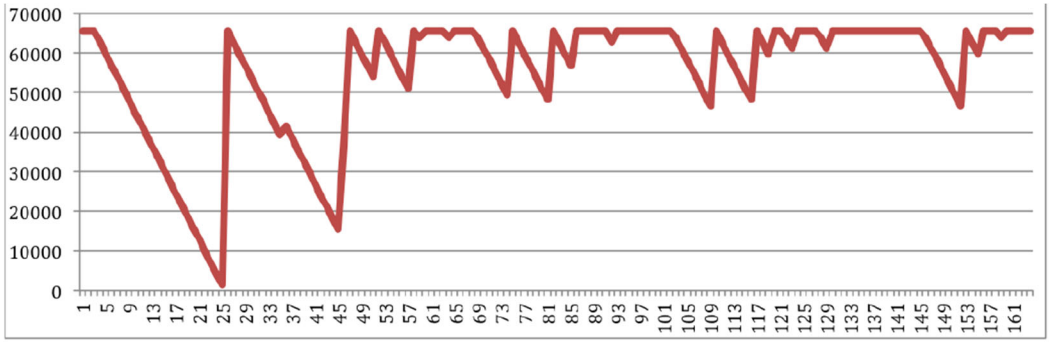


Figura 30: Grafico (numero di pacchetto - dimensione della finestra TCP) dello scaricamento del file 1 MB

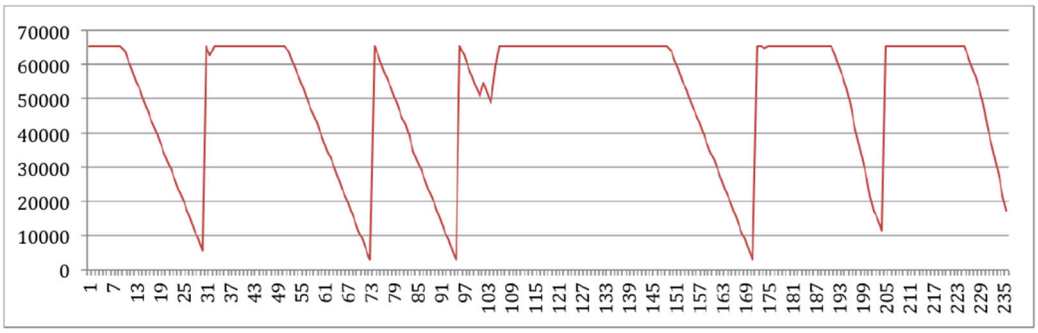


Figura 31: estratto del grafico (numero di pacchetto - dimensione della finestra TCP) dello scaricamento del file 10 MB

Esercizio 2.8

Usando JPerf si vuole confrontare il throughput UDP con quello TCP. Per poter eseguire questi test, è necessario siano presenti un processo client ed un processo server su due punti di una rete in comunicazione tra loro. JPerf può agire sia nel ruolo di client sia nel

ruolo di server, configurabile tramite semplice scelta da interfaccia grafica, ma per semplicità ci limiteremo all'uso tramite client, in quanto abbiamo attivato un server all'indirizzo 130.192.1.117, porta 5001

Per il nodo in modalità client è necessario innanzitutto impostare l'indirizzo IP del server JPerf.

Durante l'esercizio saranno da modificare di volta in volta il protocollo utilizzato (UDP o TCP), la banda massima e/o il numero di "stream paralleli" (ossia numero di connessioni in uso simultaneamente).

Dal client effettuare i seguenti test:

1. Impostare il protocollo TCP (con le opzioni di default ed il numero di "stream paralleli" a 1, svolgere il test e rilevare:

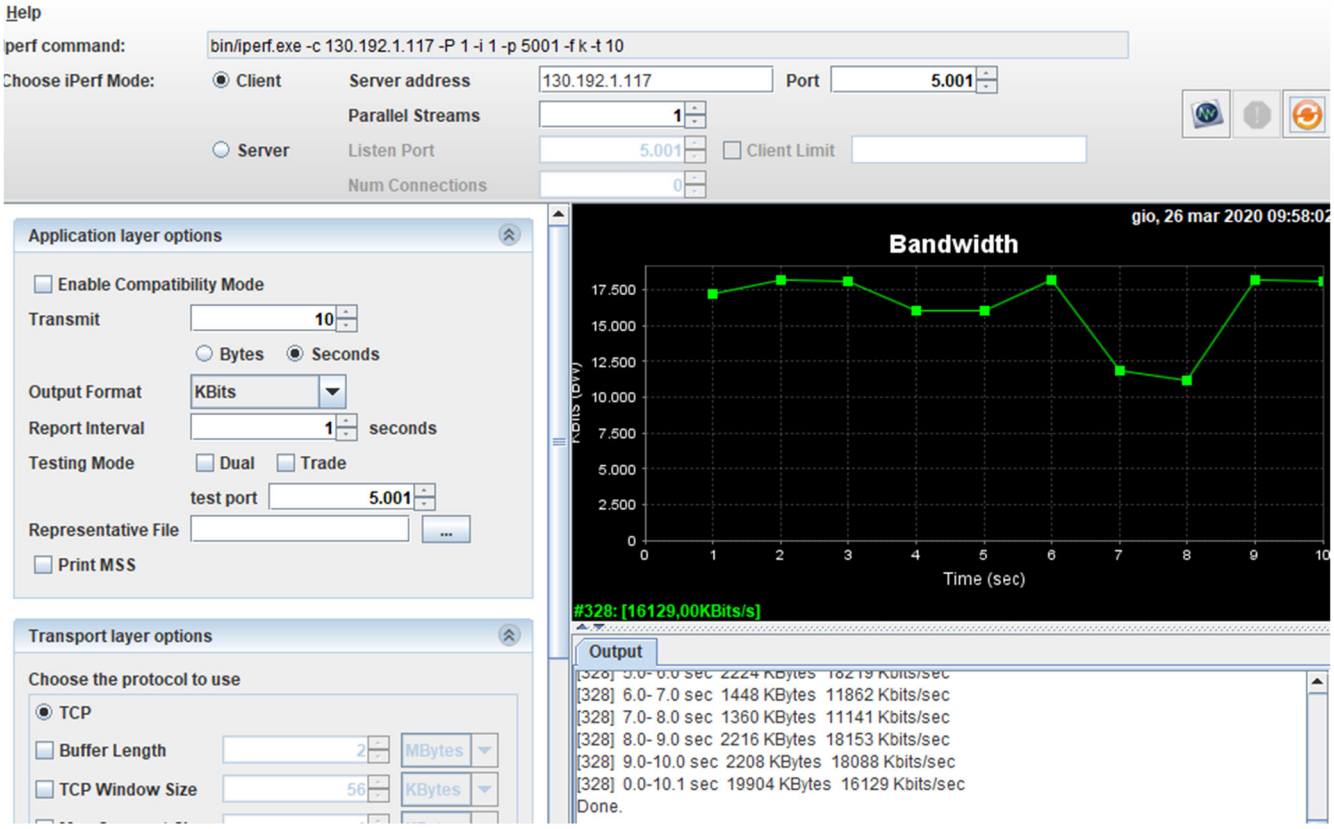


Figura 32: parametri da impostare e relativo output

Per rilevare il throughput e la percentuale di pacchetti persi è sufficiente guardare nella finestra di output del client.

2. Impostare il protocollo TCP (con le opzioni di default) ed il numero di "stream paralleli" a 5, svolgere il test e rilevare:

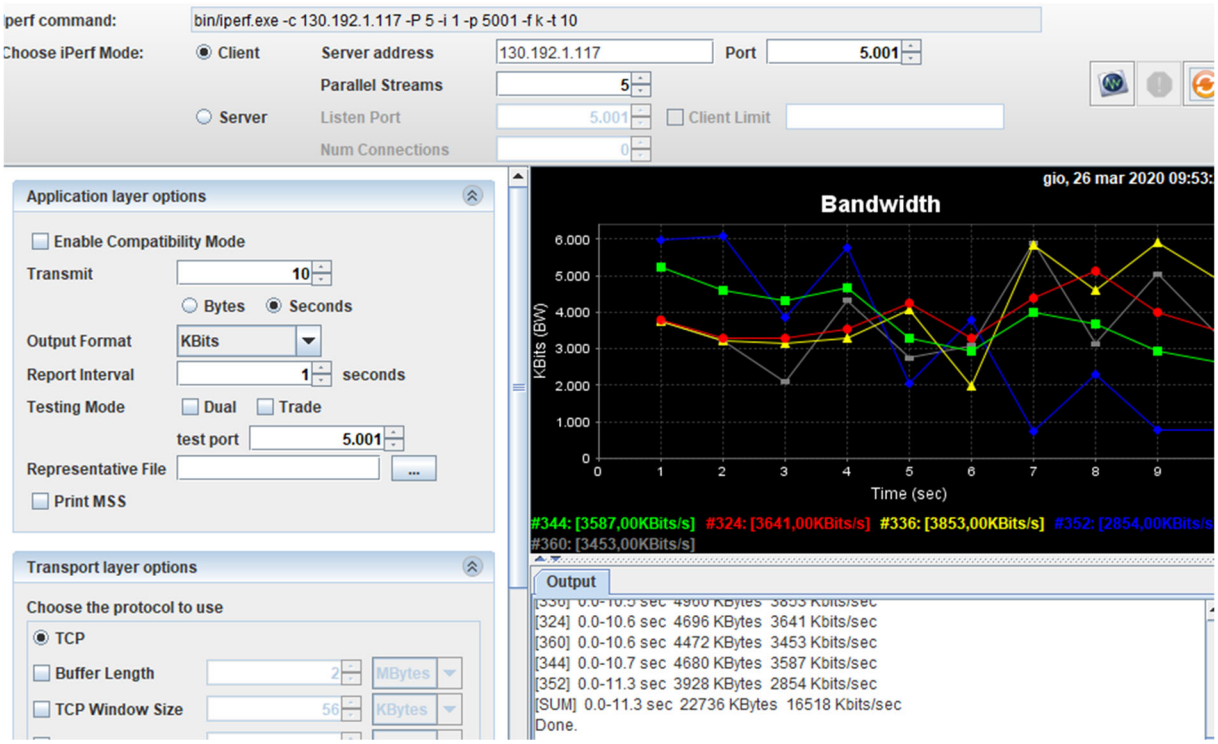


Figura 33: parametri da impostare e relativo output

Vediamo che quando ci sono flussi paralleli di dati tipicamente il throughput si abbassa.

3. Impostare il protocollo UDP, la banda ad 1 Mbps ed il numero di "stream paralleli" a 1, svolgere il test e rilevare:

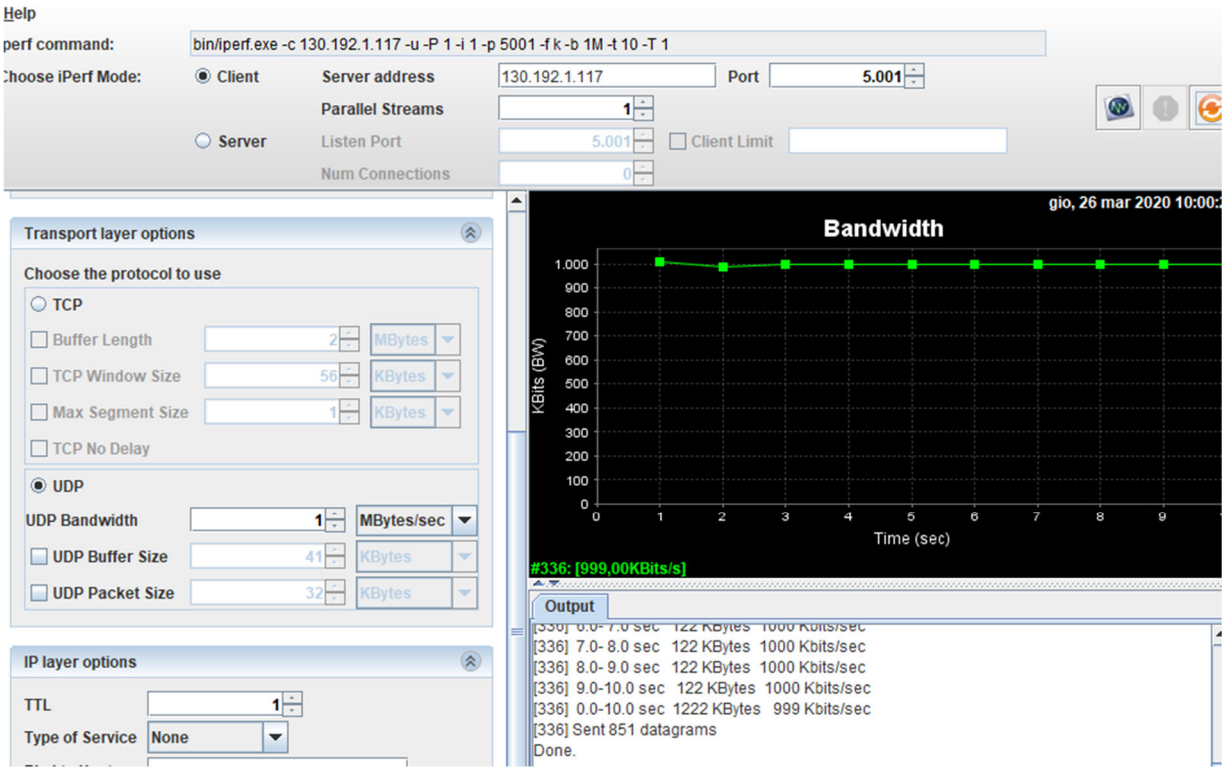


Figura 34: parametri da impostare e relativo output

4. Impostare il protocollo UDP, la banda a 5 Mbps ed il numero di "stream paralleli" a 1, svolgere il test e rilevare:

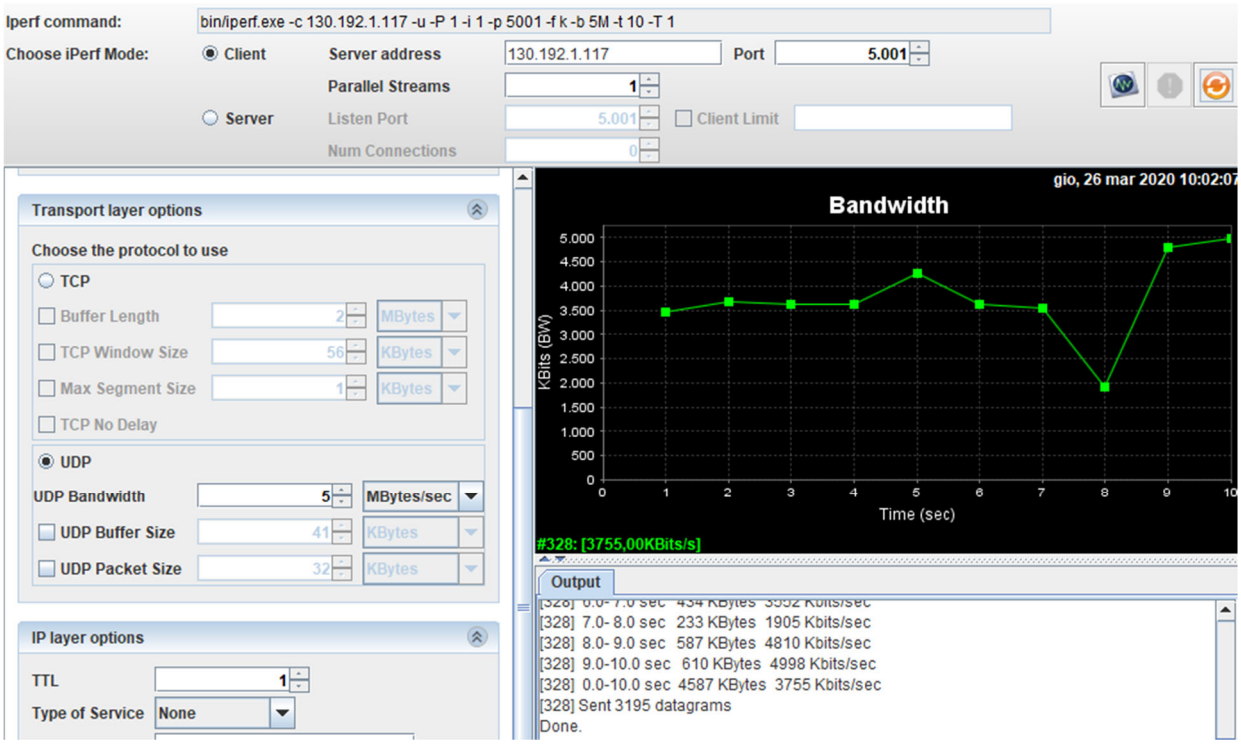


Figura 35: parametri da impostare e relativo output

5. Impostare il protocollo UDP, la banda a 10 Mbps ed il numero di "stream paralleli" a 1, svolgere il test e rilevare:

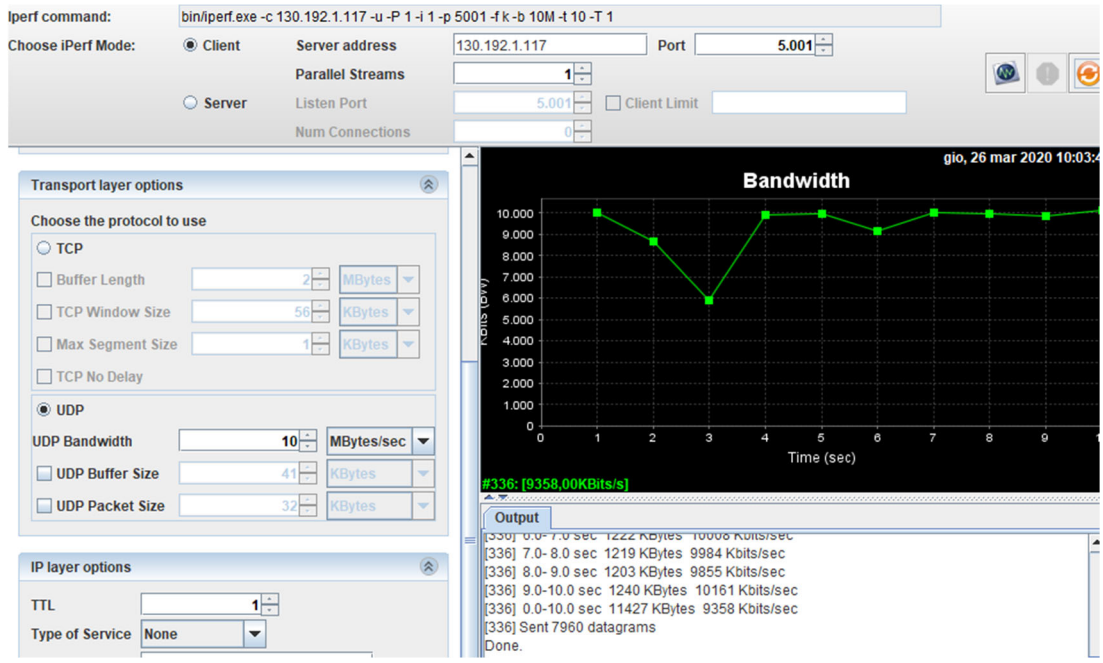


Figura 36: parametri da impostare e relativo output

6. Impostare il protocollo UDP, la banda a 1 Mbps ed il numero di "stream paralleli" a 5, svolgere il test e rilevare

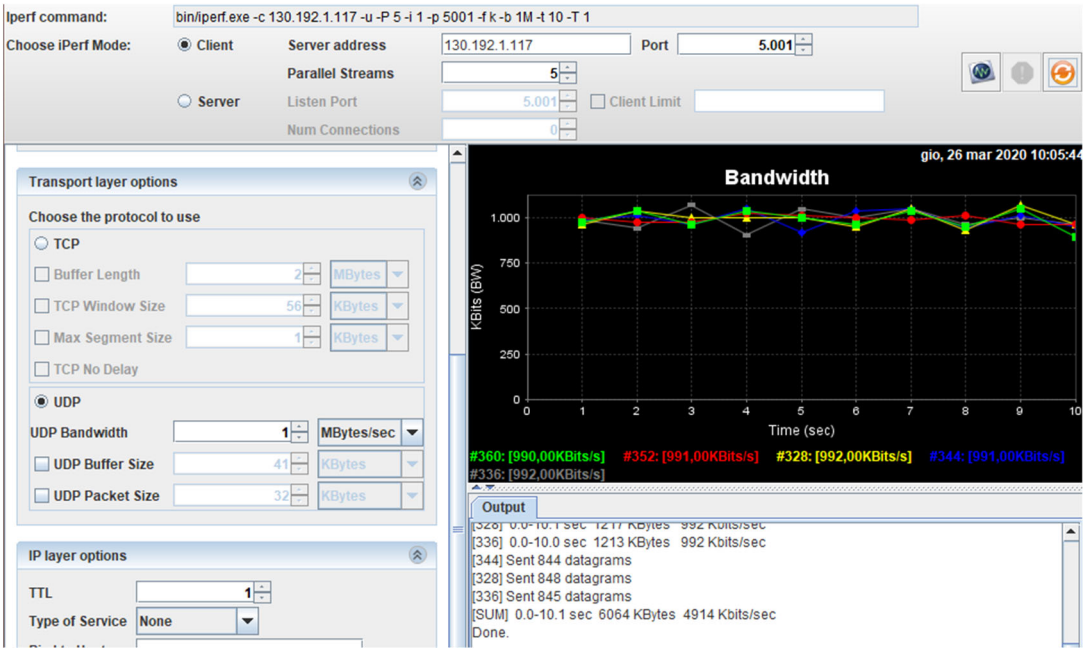


Figura 37: parametri da impostare e relativo output

7. Impostare il protocollo UDP, la banda a 5 Mbps ed il numero di "stream paralleli" a 5, svolgere il test e rilevare

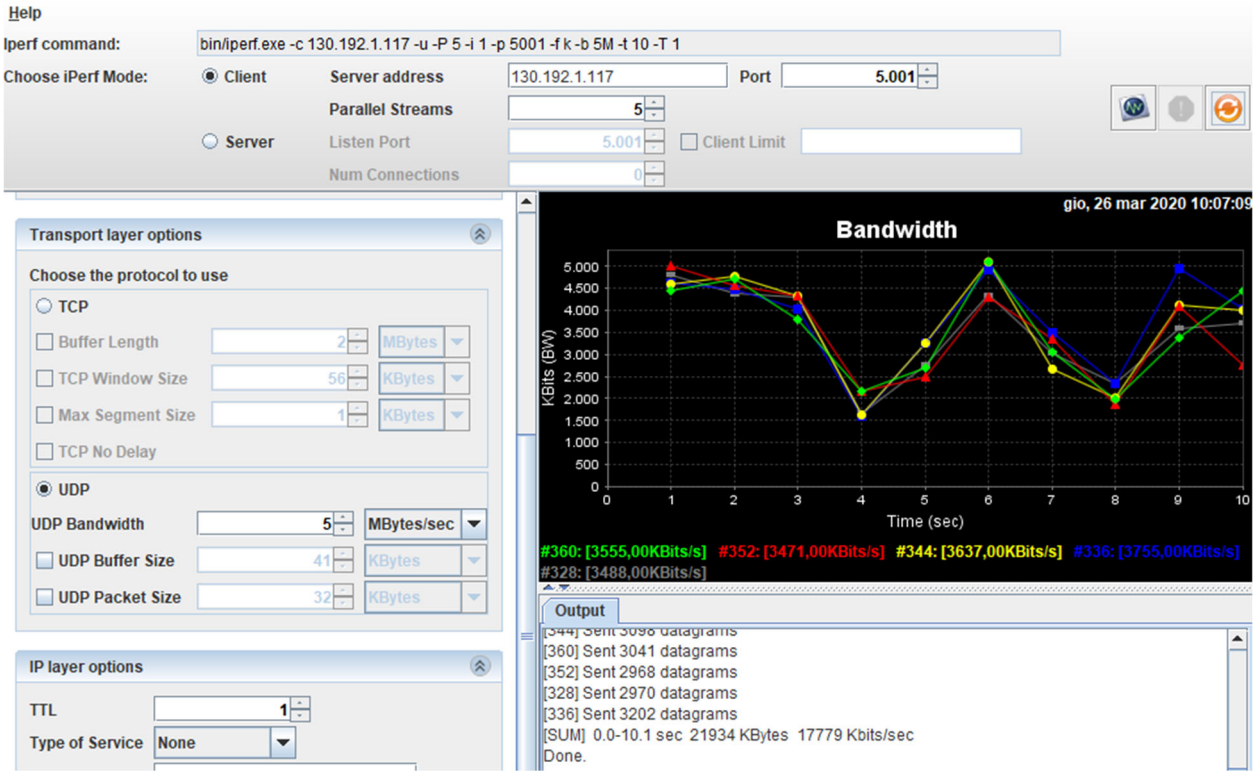


Figura 38: parametri da impostare e relativo output

8. Impostare il protocollo UDP, la banda a 10 Mbps ed il numero di "stream paralleli" a 5. Come varia il throughput rispetto al caso precedente? Ci sono pacchetti persi?

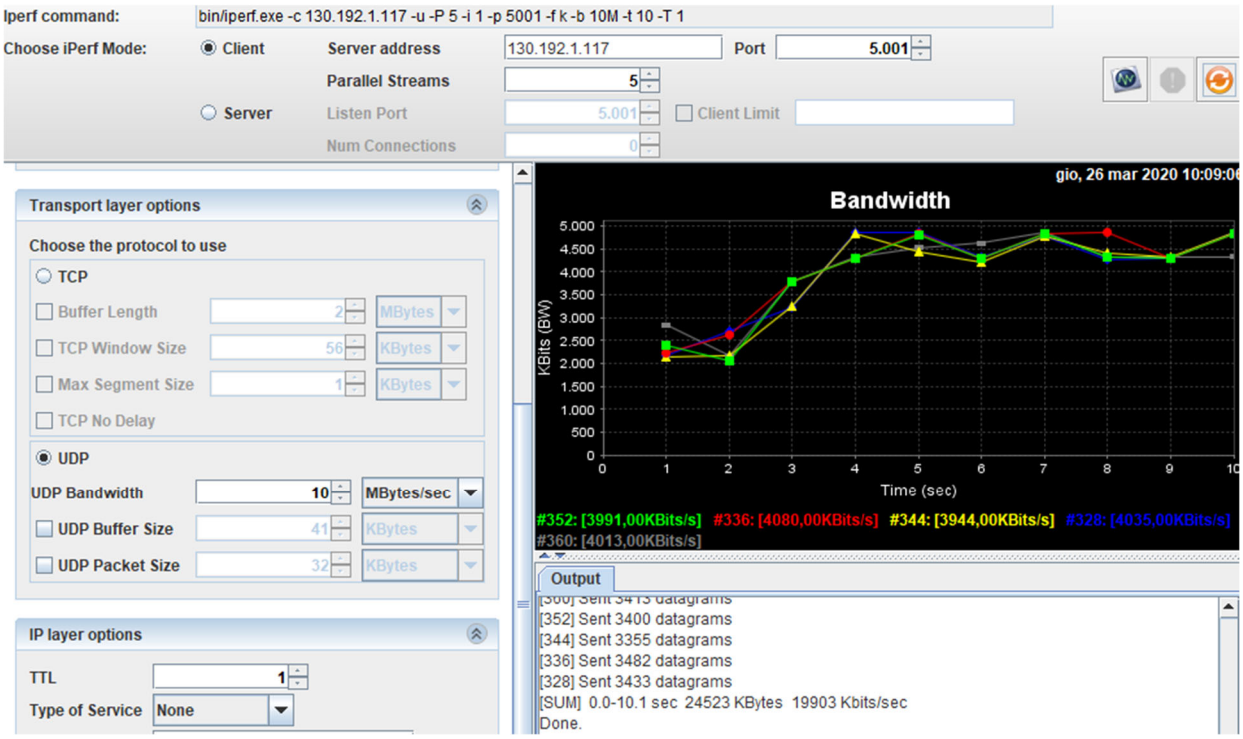


Figura 39: parametri da impostare e relativo output

Quando ci sono flussi paralleli di dati tipicamente il throughput si abbassa, infatti ci sarà un sistema di scheduling per gestire la concorrenza dei messaggi UDP.

9. Come varia il throughput al variare di protocolli e parametri del test? Ed il numero di pacchetti persi? Il throughput del protocollo UDP è superiore a quello del protocollo TCP? Analizzare i test precedenti e motivare le risposte.

Tendenzialmente quello che si nota è che, all'aumentare della dimensione del file da scaricare, il throughput aumenta. Quando invece ci sono flussi paralleli di dati tipicamente il throughput si abbassa. Questo sovraccarico rende più facile, inoltre, la perdita di datagram.

Come dimostrato da questo esercizio il throughput UDP è maggiore a quello del protocollo TCP, questo è dovuto all'assenza in UDP di molti controlli come quello di flusso e perdita di dati, che sono invece implementati in TCP. Questo permette al protocollo UDP prestazioni migliori in caso di canali con poche perdite, potendo inviare il traffico sempre alla massima velocità possibile, e per questo motivo è ancora molto utilizzato.

Appendice

L'opzione –q=A richiede il record di indirizzo. In particolare il record A identifica l'indirizzo IP versione 4, mentre il record AAAA identifica l'indirizzo IP versione 6. Inoltre è possibile richiedere i dure record contemporaneamente, specificando A+AAAA.

L'argomento "com." identifica il TLD per il qual effettuare le query. Il punto finale indica la radice (root) della gerarchia del sistema DNS. Infine il terzo parametrò è l'indirizzo IP versione 4 del "root name server" scelto per effettuare le query.

Un esempio di output ottenuto dal comando è:

```
n-addr.arpa nameserver = a.in-addr-servers.arpa

in-addr.arpa nameserver = b.in-addr-servers.arpa

in-addr.arpa nameserver = c.in-addr-servers.arpa

in-addr.arpa nameserver = d.in-addr-servers.arpa
```

```
in-addr.arpa nameserver = e.in-addr-servers.arpa
in-addr.arpa nameserver = f.in-addr-servers.arpa
a.in-addr-servers.arpa AAAA IPv6 address = 2001:500:13::73
a.in-addr-servers.arpa internet address = 199.212.0.73
b.in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
b.in-addr-servers.arpa internet address = 199.253.183.183
c.in-addr-servers.arpa AAAA IPv6 address = 2001:43f8:110::10
c.in-addr-servers.arpa internet address = 196.216.169.10
d.in-addr-servers.arpa AAAA IPv6 address = 2001:13c7:7010::53
d.in-addr-servers.arpa internet address = 200.10.60.53
e.in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::101
e.in-addr-servers.arpa internet address = 203.119.86.101
f.in-dadr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
f.in-addr-servers.arpa internet address = 193.0.9.1

Server: Unknown
Address: 198.41.0.4
Name: com

Served by:
- a.gtld-servers.net 2001:503:a83e::2:30 192.5.6.30 Com
- b.gtld-servers.net 2001:503:231d::2:30 192.33.14.30 Com
- c.gtld-servers.net 192.26.92.30 Com
- d.gtld-servers.net 192.31.80.30 Com
- e.gtld-servers.net 192.12.94.30 Com
- f.gtld-servers.net 192.35.51.30 Com
- g.gtld-servers.net 192.42.93.30 Com
- h.gtld-servers.net 192.54.112.30 Com
- i.gtld-servers.net 192.43.172.30 Com
- j.gtld-servers.net 192.48.79.30 Com
```

Si osservi che sono disponibili 10 nameserver responsabili per il TLD .com. Inoltre il comando nslookup in automatico identifica anche se per ogni server esiste l'indirizzo IP versione 6 (in questo caso solo 2 server supportano questo indirizzamento). L'opzione –q=NS richiede l'elenco dei server "authoritative" per una zona. In particolare permette di conoscere sia il nome sia l'indirizzo IP versione 4 del server.

L'argomento google.com, identifica il dominio per il quale effettuare le query. Il punto finale indica la radice (root) della gerarchia del sistema DNS. Infine il terzo parametro è l'indirizzo IP versione 4 del nameserver (responsabile per il TLD .com) scelto per effettuare le query.

Un esempio di output ottenuto dal comando è:

```
(root) nameserver = m.root-servers.net
(root) nameserver = a.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = i.root-servers.net
(root) nameserver = j.root-servers.net
(root) nameserver = k.root-servers.net
(root) nameserver = l.root-servers.net

Server: UnKnown
Address: 192.5.6.30

google.com nameserver = ns2.google.com
google.com nameserver = ns1.google.com
google.com nameserver = ns3.google.com
google.com nameserver = ns4.google.com

ns2.google.com internet address = 216.239.34.10
ns1.google.com internet address = 216.239.32.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10
```

Si osservi che sono disponibili 4 nameserver responsabili per il dominio google.com: ns1/ns2/ns3/ns4.google.com.

Inoltre, in questo caso il comando identifica sia il nome (es. ns1.google.com) che l'indirizzo IP versione 4 associato (es. 216.239.32.10). L'argomento www.google.com identifica il nome per il quale effettuare le query. Il punto finale indica la radice (root) della gerarchia del sistema DNS. Infine il terzo parametro è l'indirizzo IP versione 4 del nameserver (responsabile per il dominio google.com) scelto per effettuare le query.