

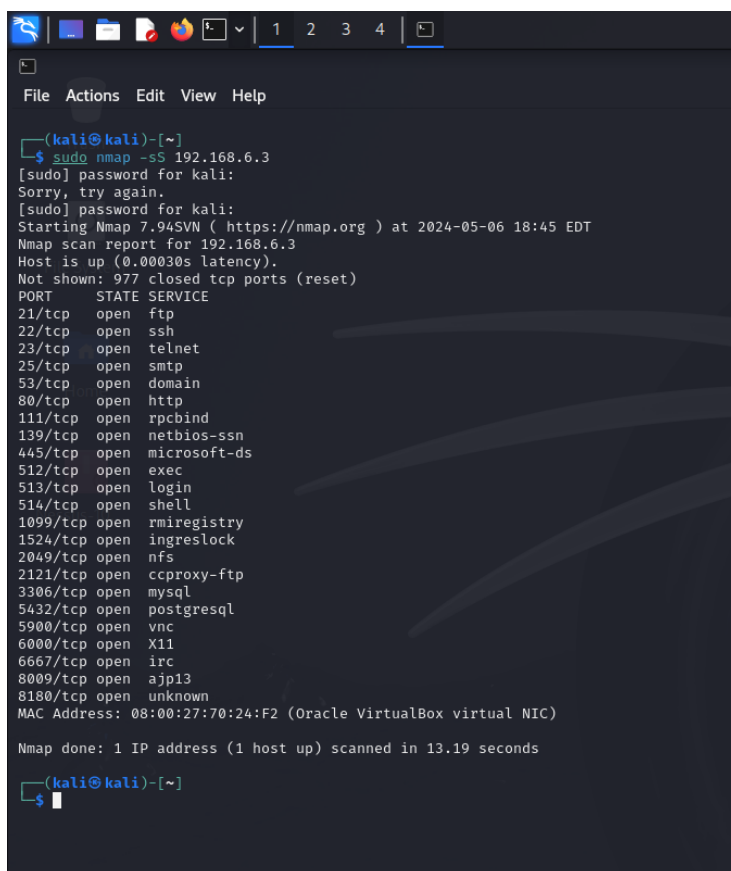
Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap. Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address
scansione senza PING: #	nmap -PN ip address

In questo esercizio scanneremo la macchina metasploitable tramite kali linux ed esamineremo ogni switch di nmap come raffigurato in tabella.

- Tcp syn scan



```

(kali@kali)-[~]
$ sudo nmap -sS 192.168.6.3
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 18:45 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
(kali@kali)-[~]
$

```

- Scansione versione dei servizi

```
(kali@kali)-[~]
└─$ sudo nmap -sV 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:01 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  cproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.01 seconds

(kali@kali)-[~]
```

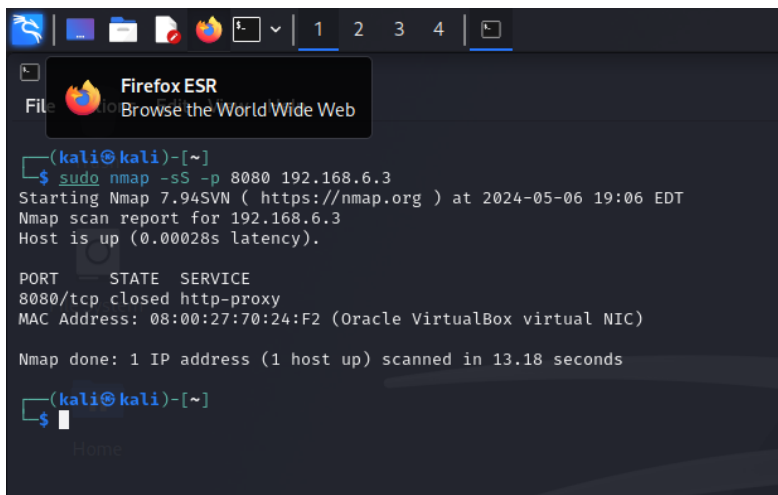
- Output su file

```
(kali@kali)-[~]
└─$ sudo nmap -sV -oN SVscan.txt 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 18:55 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
2121/tcp  open  cproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.08 seconds

(kali@kali)-[~]
```

- Scansione su porta



```
(kali@kali)-[~]
$ sudo nmap -sS -p 8080 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:06 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00028s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(kali@kali)-[~]
$
```

- Scansione su tutte le porte



```
Minimize all open windows and show the desktop
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sS -allports 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:09 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

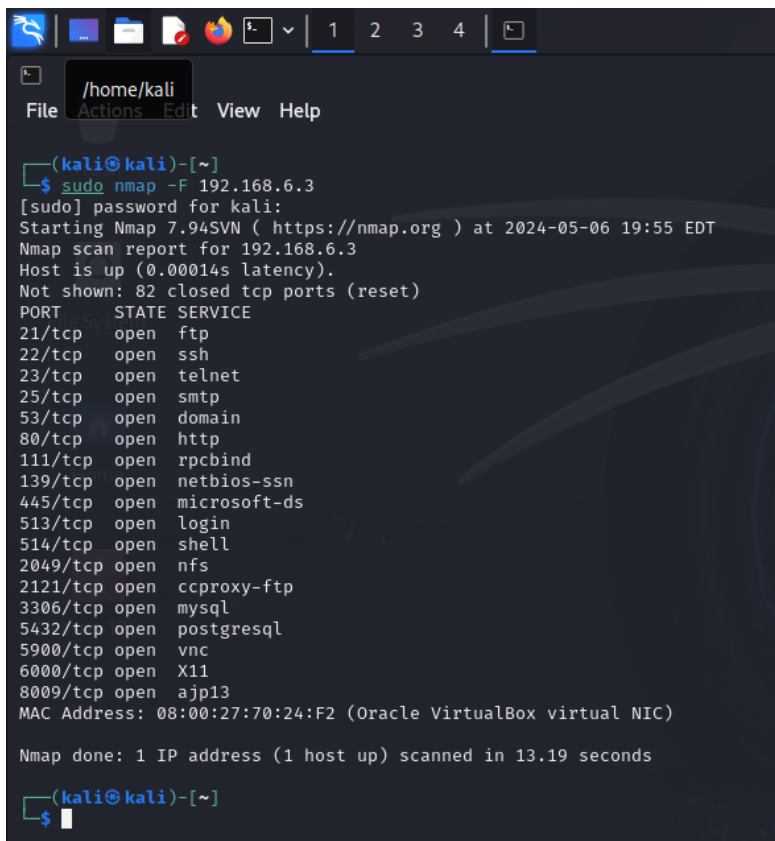
(kali@kali)-[~]
$
```

- Scansione sistema operativo

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -O 192.168.6.3
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:50 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.29 seconds
(kali@kali)-[~]
$
```

- Scansione common 100 porte



```
(kali@kali)-[~]
$ sudo nmap -F 192.168.6.3
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:55 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00014s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

(kali@kali)-[~]
$
```

- Scansione tramite arp



```
(kali@kali)-[~]
$ sudo nmap -PR 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:56 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00018s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds

(kali@kali)-[~]
$
```

- Scansione tramite ping

```

(kali@kali)-[~]
$ sudo nmap -sP 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:57 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00028s latency).
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
(kali@kali)-[~]
$

```

- Scansione senza ping

```

(kali@kali)-[~]
$ sudo nmap -PN 192.168.6.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 19:58 EDT
Nmap scan report for 192.168.6.3
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
(kali@kali)-[~]
$

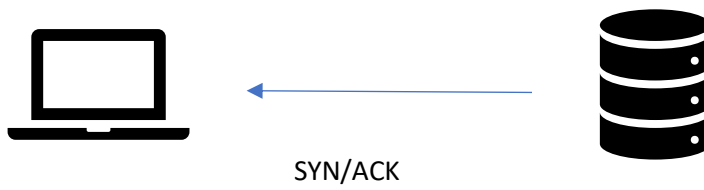
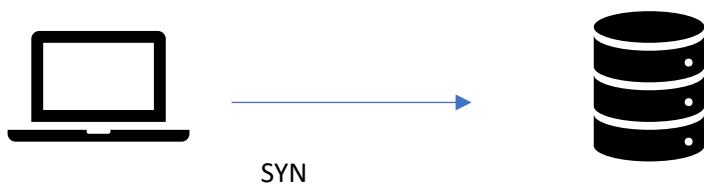
```

Grafici delle scansioni effettuate con le varie fasi di syn , syn/ack , e altri.

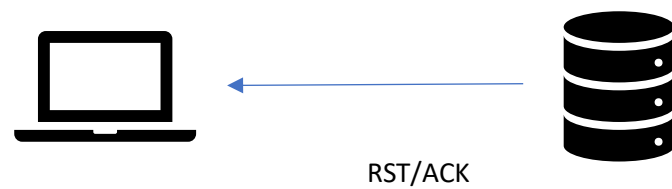
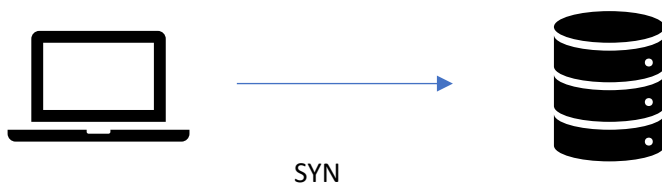
- Scansione syn : nmap -Ss indirizzo ip

Questo tipo di scansione è poco invasivo perché non completa mai le connessioni tcp.

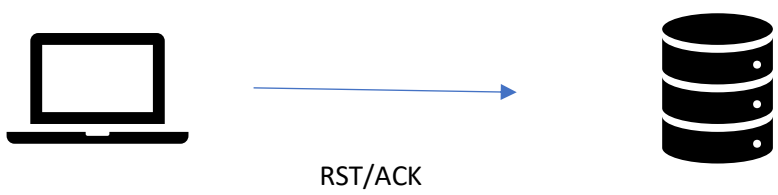
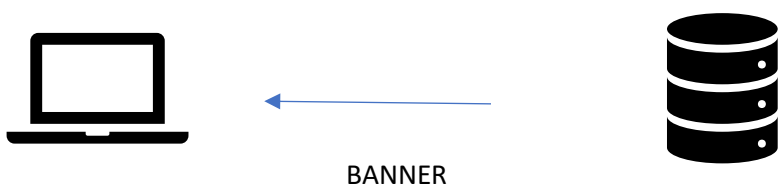
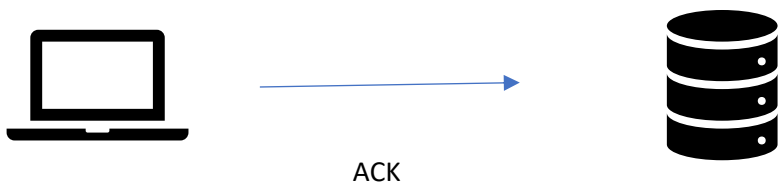
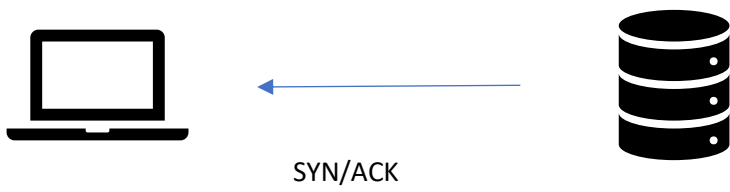
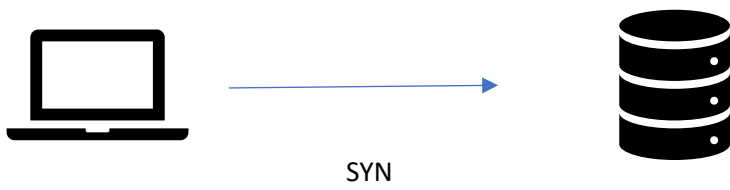
Illustreremo il grafico di una porta aperta:



- grafico di una porta chiusa:



- grafico sulla scansione di tipo versione dei servizi:



- scansione udp di una porta aperta : questo tipo di scansione è più lento e difficoltoso rispetto al TCP.

