



Lezione n.12
LPR- Informatica Applicata
Gestione della Rete

20/05/2006
Laura Ricci



INDIRIZZI RISERVATI

Alcuni indirizzi all'interno di una rete sono riservati: indirizzo di rete e broadcast. Esempio: rete 10 di classe A.

- il primo indirizzo (0) di una rete individua la rete stessa 10.0.0.0
- l'ultimo indirizzo individua tutti gli host di quella rete (broadcast) 10.255.255.255
- indirizzi
 - Privati non utilizzato in internet. Può essere utilizzato in reti non collegate
 - Pubblico: utilizzato direttamente ad internet

IL COMANDO IFCONFIG (IPCONFIG WINDOWS)

- mostra lo stato di una interfaccia di rete (eth0-ethernet0, eth1-ethernet1, lo-loopback,...) o di tutte (se non specifico parametri)
- assegna ad una interfaccia di rete un indirizzo IP

ifconfig eth0

```
Link encap:Ethernet HWaddr 52:54:00:EB:EC:C6
inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:82075264 errors:0 dropped:0 overruns:0 frame:0
TX packets:51585638 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
Interrupt:10 Base address:0xb800
```

IL COMANDO IFCONFIG

ifconfig lo

Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.255.255.0

UP LOOPBACK RUNNING MTU:1500 Metric:1

RX packets:10226970 errors:0 dropped:0 overruns:0 frame:0

TX packets:10226970 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

E' possibile associare un indirizzo IP ad una interfaccia

```
ifconfig eth0 192.168.1.100
```

ASSOCIAZIONE SERVIZI-PORTE

In LINUX, il file `/etc/services` elenca le porte dei servizi noti

```
ftp-data      20/tcp
ftp-data      20/udp # 21 is registered to ftp,
            but also used by fsp
ftp           21/tcp
ftp           21/udp      fsp fspd
ssh 22/tcp    # SSH Remote Login Protocol
ssh 22/udp    # SSH Remote Login Protocol
telnet        23/tcp
telnet        23/udp
smtp          25/tcp mail
smtp          25/udp mail
```

IL COMANDO PING

ping <host>

- controlla se l'host <host> è raggiungibile
- registra il round trip-time tra il richiedente ed <host>

```
# ping -s 300 -c 10 qua.di.unipi.it
```

```
PING qua.di.unipi.it (131.114.4.118): 300 data bytes
```

```
308 bytes from 131.114.4.118: icmp_seq=1 ttl=52 time=290.0 ms
```

```
308 bytes from 131.114.4.118: icmp_seq=4 ttl=52 time=280.0 ms
```

```
308 bytes from 131.114.4.118: icmp_seq=7 ttl=52 time=280.0 ms
```

```
308 bytes from 131.114.4.118: icmp_seq=8 ttl=52 time=300.0 ms
```

```
--- qua.di.unipi.it ping statistics ---
```

```
10 packets transmitted, 4 packets received, 60% packet loss
```

```
round-trip min/avg/max = 280.0/287.5/300.0 ms
```

- c num termina dopo aver ricevuto num risposte
- s size invia pacchetti di dimensione size, (valore di default di 56 bytes)



IL COMANDO PING: COSA RILEVA

- il mittente
 - genera una sequenza di **echo request**, con una frequenza di 1 pacchetto ICMP al secondo
 - associa un numero di sequenza unico ed un timestamp ad ogni pacchetto trasmesso
- il destinatario riceve il pacchetto e genera un **echo-reply**
- in base ai numeri di sequenza degli echo-replay ricevuti, il mittente determina quanti e quali pacchetti sono persi, quanti duplicati, quanti riordinati
- può individuare, mediante checksum, i pacchetti danneggiati
- determina sulla base del timestamp contenuto nell'echo replay, il Round Trip Time (RTT), cioè il tempo di scambio dei pacchetti.

IL COMANDO PING: COSA NON PUO' RILEVARE

- può restituire il messaggio "host unreachable", ma non ne individua la causa
 - l'host potrebbe essere spento
 - ci possono essere problemi di raggiungibilità della rete
 - un firewall potrebbe aver filtrato i pacchetti ICMP
- non individua il motivo per cui un pacchetto è stato danneggiato, duplicato, riordinato
- registra il tempo intercorso tra la richiesta e la risposta, ma questo tempo è solo indicativo delle condizioni della rete
 - comprende il tempo di attraversamento dei routers (pacchetti ICMP possono avere bassa priorità di instradamento all'interno dei routers)

IL COMANDO PING: OPZIONI

```
#ping -n 192.168.98.254
```

controllare la raggiungibilità dell' host con l'indirizzo IP assegnato.
-n evita di risolvere i nomi simbolici tramite DNS.

```
#ping -i 3 192.168.98.254
```

-i x aspetta x secondi invece di uno tra la trasmissione di un pacchetto ed il successivo

```
#ping -p A3B567CD2
```

-p pattern specifica il valore (codificato in esadecimale) del payload del pacchetto. Si può utilizzare per diagnosticare eventuali corruzioni di dati

IL COMANDO PING: FLOOD PING

```
#ping -f 192.168.168.10
```

-f flood ping

il numero di echo requests da inviare per ogni secondo viene stabilito in base al tempo di ricezione degli echo-reply. Vengono comunque spediti almeno 100 pacchetti al secondo.

```
#ping -c 400 -f -n 192.168.99.254
```

```
PING 192.168.99.254 (192.168.99.254) from 192.168.98.82: 56(84) bytes of data
```

```
.....
```

```
---192.168.99.254 ping statistics---
```

```
411 packets transmitted, 400 packets received, 2% packet loss
```

```
Round-trip min/avg/max/mdev = 37.840/62.234/97.807/12.946 ms
```



IL COMANDO PING: OPZIONI

Posso aumentare la dimensione del pacchetto per verificare la reazione della rete

```
#ping -s 512 -c 400 -f -n 192.168.99.254
PING 192.168.99.254 (192.168.99.254) from 192.168.98.82: 512(540) bytes of data
.....
---192.168.99.254 ping statistics---
511 packets transmitted, 400 packets received, 27% packet loss
round-trip min/avg/max/mdev = 47.854/295.711/649.595/153.345 ms
```



IL COMANDO TRACEROUTE (TRACERT WINDOWS)

tracert terp.umd.edu

```
tracert to terp.umd.edu (128.8.10.90), 30 hops max, 40 byte packets
 1  cisco (199.2.50.1)          3.08 ms  2.391 ms  2.653 ms
 2  sl-stk-3-S17-128k.sprintlink.net (144.228.202.1) 232.955 ms 195.828
    ms 309.079 ms
 3  sl-stk-5-F0/0.sprintlink.net (144.228.40.5) 187.623 ms *
    24.545 ms
 4  icm-fix-w-H2/0-T3.icp.net (144.228.10.22) 28.927 ms 27.511 ms
    34.684 ms
 5  fix-west-cpe.SanFrancisco.mci.net (192.203.230.18) 124.641 ms
    225.516 ms *
 6  border3-hssi2-0.SanFrancisco.mci.net (204.70.34.9) 127.727 ms
    29.322 ms 30.108 ms
 7  core-fddi-0.SanFrancisco.mci.net (204.70.2.161) 227.059 ms 112.441
    ms 29.868 ms
 8  core-hssi-2.Denver.mci.net (204.70.1.37) 52.881 ms 53.632 ms
    53.18 ms
 9  core-hssi-3.Washington.mci.net (204.70.1.13) 93.393 ms 120.491
    ms 92.691 ms
10  border1-fddi0-0.Washington.mci.net (204.70.2.2) 242.042 ms 94.312
    ms 265.366 ms
```



IL COMANDO TRCERROUTE (TRACERT IN WINDOWS)

```
11  suranet-cpe.Washington.mci.net (204.70.56.6)          193.482 ms
    * 93.427 ms
12  wtn8-wtn-cf.sura.net (128.167.7.8)          105.636 ms  92.919 ms
    93.663 ms
13  sura9-wtn8-c3.sura.net (128.167.212.1)       92.88 ms
    92.708 ms  98.033 ms
14  sura2-sura-ce.sura.net (128.167.1.2)         105.182 ms  115.759
    ms *
15  umd-sura2-c1.sura.net (192.221.61.2)        132.248 ms  145.699
    ms 182.908 ms
16  csclhub-gw.umd.edu (128.8.1.224)           168.827 ms  * *
17  terp.umd.edu (128.8.10.90)                 118.98 ms  156.011 ms
    160.125 ms
```



IL COMANDO TRACEROUTE: IMPLEMENTAZIONE

- invia una sequenza di pacchetti UDP con valore di TTL crescente
- invia tre pacchetti per ogni valore del TTL
- riceve un **ICMP time exceeded** da ogni router attraversato per giungere a destinazione
- ricava le informazioni sui routers attraversati dai pacchetti ICMP ricevuti

IL COMANDO TRACEROUTE

traceroute term.umd.edu

```
traceroute to terp.umd.edu (128.8.10.90), 30 hops max, 40
  byte packets
 1  cisco (199.2.50.1) 3.08 ms 2.391 ms 2.653 ms
 2  sl-stk-3-S17-128k.sprintlink.net (144.228.202.1)
    232.955ms195.828 ms309.079ms
 3  sl-stk-5-F0/0.sprintlink.net (144.228.40.5) 187.623 ms
    * 24.545 ms
 4  icm-fix-w-H2/0-T3.icp.net (144.228.10.22) 28.927 ms
    27.511 ms 34.684 ms
 5  fix-west-cpe.SanFrancisco.mci.net (192.203.230.18) 124.641
    ms 225.516 ms *
```

ogni riga di output contiene

- il nome simbolico del router (determinato dal DNS)
- l'indirizzo IP
- i tre valori del round trip time per i tre pacchetti spediti per ogni TTL
- un asterisco indica che l'host non ha risposto al pacchetto corrispondente



IL COMANDO NETSTAT

- permette di visualizzare tutte le porte aperte su un host
- mostra le informazioni relative a tutti i socket aperti (anche i collegamenti usati da processi locali per scambiarsi i dati mediante sockets)
- -t visualizza solo i socket TCP
- -u visualizza solo i socket UDP
- -n non interroga il DNS
- -a mostra sia le porte in attesa di connessione che quelle attive

IL COMANDO NETSTAT

<i>Proto</i>	<i>Recv-Q</i>	<i>Send-Q</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
tcp	0	0	12.123.45.67.50033	195.22.198.15.80	ESTABLISHED
tcp	0	0	192.168.0.1.65232	217.220.29.16.6667	ESTABLISHED
tcp	0	0	192.168.0.1.65231	213.92.8.4.6667	ESTABLISHED
tcp	0	0	192.168.0.1.139	*.*	LISTEN
tcp	0	0	127.0.0.1.3493	127.0.0.1.49154	ESTABLISHED
tcp	0	0	*.3493	*.*	LISTEN
tcp	0	0	*.80	*.*	LISTEN
tcp	0	0	*.25	*.*	LISTEN
tcp	0	0	*.22	*.*	LISTEN

Proto = protocollo

Recv-Q, Send-Q = numero di pacchetti sulle porte di ricezione/invio

Local Address= indirizzo e porta locali. Un asterisco al posto dell'indirizzo IP indica che la porta è attiva su ogni indirizzo locale

Foreign Address = indirizzo e porta remoti *.* se in attesa di connessioni

State = stato (in attesa di connessione, connessione stabilita,...)



IL COMANDO NETSTAT

Stati di una sessione

LISTEN = in attesa di connessioni

ESTABLISHED = connessione attiva

SYN_SENT = connessione TCP richiesta dall'host locale

SYN_RECV = connessione TCP richiesta da un host remoto

TIME_WAIT = la connessione è stata chiusa, ma il kernel
sta attendendo gli ultimi pacchetti in transito
sulla rete

.....