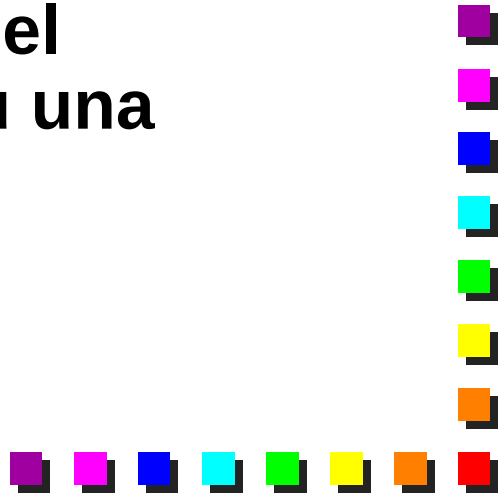
Strumenti per analisi di rete

Una panoramica sui principali strumenti per la verifica del comportamento della rete su una workstation



Attenzione...

- I comandi presenti in questo file sono normalmente presenti sia in ambito UNIX che in ambito Windows
- Tuttavia...
  - Non sempre questo è vero
  - Non sempre hanno esattamente le stesse opzioni
  - Non sempre hanno esattamente lo stesso output
- Pertanto…
  - Questo elenco di comandi deve essere inteso come “indicativo”, e sarà necessario effettuare l’opportuna verifica dell’esistenza dei comandi / opzioni sul sistema operativo desiderato
- Inoltre…
  - Per ogni comando si elencano solo le opzioni che si ritengono essere più importanti

Ping

- Verifica che un host remoto sia attivo a livello rete
- Sintassi:

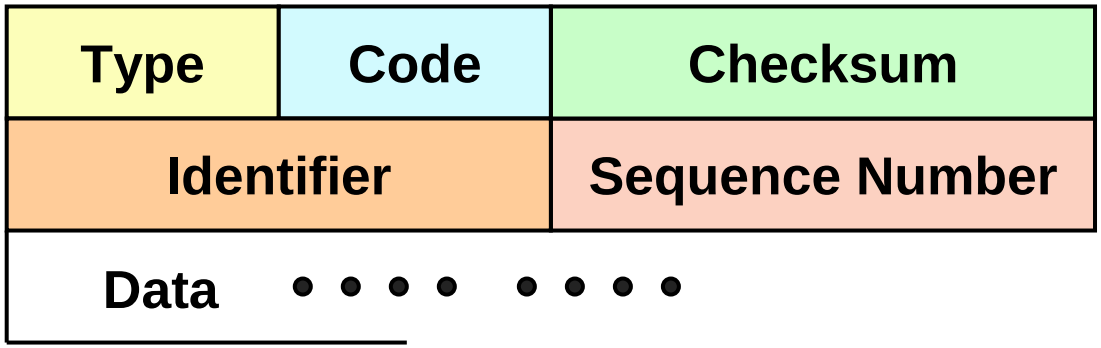
```
ping [opzioni] destinazione
```

Opzione	Descrizione
`-t`	Continua ad inviare pacchetti ICMP Echo Request fino a quando non viene interrotto manualmente con un Ctrl+C (solo in Windows; in UNIX questo è il comportamento di default).
`-c count`	Invia `count` pacchetti ICMP Echo Request (Windows ha di default `count` pari a 4).
`-i TTL`	Spedisce i pacchetti ICMP Echo Request con il valore del campo Time To Live pari a `TTL` (solo Windows).
`-w timeout`	Aspetta ogni risposta per max `timeout` millisecondi. Se la risposta arriva più tardi, viene ignorata.
`-R`	Memorizza il percorso seguito, attivando l'opzione *Record Route* nel pacchetto di ICMP Echo Request.

Ping: funzionamento

- **Messaggi**
  - L'host che effettua il test invia un messaggio `ICMP Echo Request`
  - L'host sotto test risponde inviando un messaggio `ICMP Echo Reply`

0 = Echo Request
8 = Echo Reply



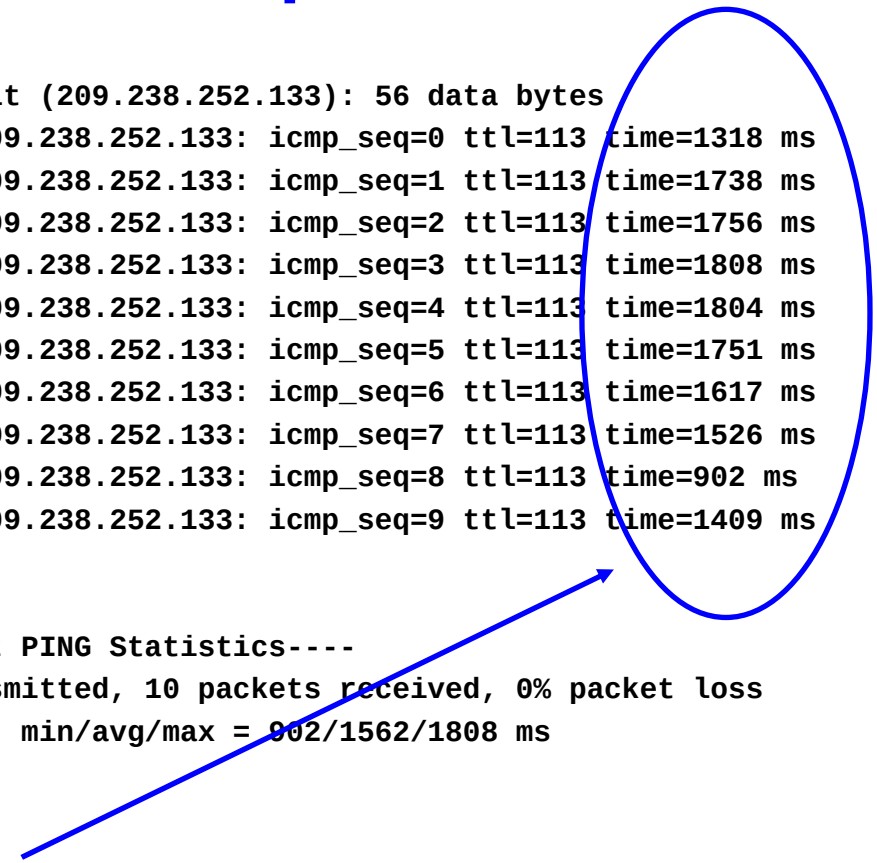
Ping: risultati

- Se il PING ha esito positivo, tutto è OK
- Se il PING fallisce, non ci sono molte indicazioni su quanto è successo
  - Potrebbe esserci un problema sul percorso di andata verso l'host sotto test
  - Potrebbe esserci un problema sul percorso di ritorno dall'host sotto test verso l'host che effettua il test
    - In Internet non c'è nessuna garanzia che i percorsi siano simmetrici
  - Potrebbe esserci un'Access-List sui router o firewall intermedi che inibiscono il protocollo ICMP
  - Potrebbe esserci un Personal Firewall attivato sull'host sotto test
    - Spesso i Personal Firewall disabilitano le risposte ICMP

Esempio di output

```
PING www.xenia.it (209.238.252.133): 56 data bytes
64 bytes from 209.238.252.133: icmp_seq=0 ttl=113 time=1318 ms
64 bytes from 209.238.252.133: icmp_seq=1 ttl=113 time=1738 ms
64 bytes from 209.238.252.133: icmp_seq=2 ttl=113 time=1756 ms
64 bytes from 209.238.252.133: icmp_seq=3 ttl=113 time=1808 ms
64 bytes from 209.238.252.133: icmp_seq=4 ttl=113 time=1804 ms
64 bytes from 209.238.252.133: icmp_seq=5 ttl=113 time=1751 ms
64 bytes from 209.238.252.133: icmp_seq=6 ttl=113 time=1617 ms
64 bytes from 209.238.252.133: icmp_seq=7 ttl=113 time=1526 ms
64 bytes from 209.238.252.133: icmp_seq=8 ttl=113 time=902 ms
64 bytes from 209.238.252.133: icmp_seq=9 ttl=113 time=1409 ms


----www.xenia.it PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 902/1562/1808 ms
```



Round-trip time (RTT): **tempo da quando è stato generato il pacchetto ICMP Echo Request a quando è stato ricevuto il pacchetto ICMP Echo Reply; è un'indicazione della "*distanza*" esistente tra i due host.**

Traceroute (1)

- Visualizza il (presunto) percorso verso l'host destinazione
  - individua i router che vengono attraversati tra la stazione che effettua il test e la stazione terminale di destinazione
  - ATTENZIONE: ogni router risponde con UNO dei suoi indirizzi IP, non necessariamente quello dell'interfaccia sul percorso tra la sorgente e la destinazione
- Sintassi:

```
traceroute [opzioni] destinazione (UNIX)
tracert [opzioni] destinazione (Windows)
```

- UNIX: alcune implementazioni inviano un pacchetto UDP anzichè ICMP

Traceroute (2)

Opzione	Descrizione
`-f TTL`	Utilizza il valore `TTL` come valore iniziale del campo Time To Live del pacchetto IP (anzichè partire da uno).
`-l`	Utilizza pacchetti ICMP Echo Request anzichè pacchetti UDP (solo UNIX).
`-p port`	Genera pacchetti UDP con porta destinazione pari a `port` anzichè il valore di default 33434 (solo UNIX).
`-m count`	Utilizza, come massimo valore del campo Time To Live del pacchetto IP, il valore `count` (default 30).
`-w timeout`	Aspetta ogni risposta per max `timeout` millisecondi. Se la risposta arriva più tardi, viene ignorata.
`-q count`	Genera `count` pacchetti di test per ogni valore di Time To Live (default tre).

Traceroute: funzionamento

- Fasi della sequenza di pacchetti del programma Traceroute
  1. La stazione che effettua il test invia un messaggio `ICMP Echo Request` con TTL = 1 al default gateway
  2. Il primo router scarta il messaggio e risponde inviando un messaggio `ICMP TTL Exceeded in Transit`
  3. La stazione che effettua il test invia apprende l'esistenza del primo router e invia un successivo messaggio `ICMP Echo Request` con TTL incrementato di 1 al default gateway (TTL = 2)
  4. Il default gateway inoltra il messaggio al router successivo decrementando il TTL
  5. Il secondo router scarta il messaggio e risponde inviando un messaggio `ICMP TTL Exceeded in Transit`

Esempio di output

```
traceroute to library.airnews.net (206.66.12.202), 30 hops max, 40 byte packets
  1  rbrt3 (208.225.64.50)  4.867 ms  4.893 ms  3.449 ms
  2  519.Hssi2-0-0.GW1.EWR1.ALTER.NET (157.130.0.17)  6.918 ms  8.721 ms  16.476 ms
  3  113.ATM3-0.XR2.EWR1.ALTER.NET (146.188.176.38)  6.323 ms  6.123 ms  7.011 ms
  4  192.ATM2-0.TR2.EWR1.ALTER.NET (146.188.176.82)  6.955 ms  15.400 ms  6.684 ms
  5  105.ATM6-0.TR2.DFW4.ALTER.NET (146.188.136.245)  49.105 ms  49.921 ms  47.371 ms
  6  298.ATM7-0.XR2.DFW4.ALTER.NET (146.188.240.77)  48.162 ms  48.052 ms  47.565 ms
  7  194.ATM9-0-0.GW1.DFW1.ALTER.NET (146.188.240.45)  47.886 ms  47.380 ms  50.690 ms
  8  iadfw3-gw.customer.ALTER.NET (137.39.138.74)  69.827 ms  68.112 ms  66.859 ms
  9  library.airnews.net (206.66.12.202)  174.853 ms  163.945 ms  147.501 ms
```

Round-trip time (RTT): tempo calcolato dall'invio del pacchetto ICMP alla ricezione del pacchetto ICMP Time Exceedded; è possibile visualizzare, in maniera molto approssimata, i tempi di percorrenza tra l'host in esame e ogni singolo router.
Spesso è possibile verificare come ci siano forti variazioni di tempo di risposta a distanza di pochi secondi.

ARP

- Visualizza e modifica il contenuto dell'ARP cache
- Sintassi:

```
arp [opzioni] [IPAddr] [EthAddr]
```

Opzione	Descrizione
`-a`	Visualizza l'attuale stato dell'ARP cache, distinguendo tra valori statici e dinamici.
`-d IPAddr`	Cancella dall'ARP cache l'associazione relativa all'host `IPAddr`.
`-s IPAddr EthAddr`	Aggiunge una associazione statica tra l'indirizzo di livello tre `IPAddr` e l'indirizzo di livello due `EthAddr`.

Esempio di output

```
C:\>arp –a

Interface: 130.192.16.81 --- 0x30004
  Internet Address      Physical Address      Type
  130.192.16.17         00-e0-63-13-7e-01     dynamic
  130.192.16.36         00-10-4b-35-f2-fa     dynamic
```

Netstat

- Visualizza i principali parametri relativi allo stato della rete sulla stazione in esame
- Sintassi:

```
netstat [opzioni]
```

Opzione	Descrizione
`[no param.]`	Visualizza l'elenco delle connessioni di livello 4 attualmente attive.
`-a`	Visualizza sia le connessioni di livello 4 attualmente attive, sia i server in ascolto su una qualunque porta TCP o UDP sulla macchina in esame.
`-s`	Visualizza le statistiche per protocollo (di livello 3 e 4).
`-e`	Visualizza le statistiche relative alla scheda Ethernet.
`-r`	Visualizza la routing table.

Esempio di output (1)

```
C:\>netstat –a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    truciolo:http          truciolo:0             LISTENING
  TCP    truciolo:epmap         truciolo:0             LISTENING
  TCP    truciolo:https         truciolo:0             LISTENING
  TCP    truciolo:2747          truciolo:0             LISTENING
  TCP    truciolo:2747          localhost:2748         ESTABLISHED
  TCP    truciolo:2748          localhost:2747         ESTABLISHED
  UDP    truciolo:microsoft-ds  *:*
  UDP    truciolo:isakmp        *:*
  UDP    truciolo:1030          *:*
  UDP    truciolo:1078          *:*
  UDP    truciolo:2040          *:*
  UDP    truciolo:2359          *:*
  UDP    truciolo:3456          *:*
  UDP    truciolo:4500          *:*
  UDP    truciolo:ntp           *:*
```

Esempio di output (2)

```
C:\>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 10 4b 35 f2 fa ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     130.192.3.17    130.192.28.4       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      130.192.0.0      255.255.0.0     130.192.28.4    130.192.28.4       1
     130.192.28.4  255.255.255.255        127.0.0.1       127.0.0.1       1
  130.192.255.255  255.255.255.255     130.192.28.4    130.192.28.4       1
        224.0.0.0        224.0.0.0     130.192.28.4    130.192.28.4       1
  255.255.255.255  255.255.255.255     130.192.28.4    130.192.28.4       1
Default Gateway:      130.192.3.17
===========================================================================
Persistent Routes:
  None
```

Esempio di output (3)

```
C:\>netstat -s

IPv4 Statistics
  Packets Received                    = 1762191
  Received Header Errors              = 12
  Received Address Errors             = 655093
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 1127699
  Output Requests                     = 951452
  Routing Discards                    = 0
  Discarded Output Packets            = 0
  Output Packet No Route              = 8
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0

[continue ...]
```

```
[...continue]

ICMPv4 Statistics
                            Received    Sent
  Messages                  1246        1780
  Errors                    0           0
  Destination Unreachable   371         476
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     555         749
  Echo Replies              168         555
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4
  Active Opens                        = 8767
  Passive Opens                       = 769
  Failed Connection Attempts          = 420
  Reset Connections                   = 1436
  Current Connections                 = 3
  Segments Received                   = 759943
  Segments Sent                       = 768276
  Segments Retransmitted              = 1003
```

Esempio di output (4)

```
C:\>netstat -e

Interface Statistics

                           Received            Sent

Bytes                     458905257       313090297
Unicast packets              786574          805622
Non-unicast packets         1565173           34366
Discards                          0               0
Errors                            0             112
Unknown protocols            232253               0
```

Route

- Visualizza e modifica la routing table
- Sintassi:

```
route [opzioni] [commando] [parametri]
```

Opzione	Descrizione
`print`	Visualizza la routing table; equivalente a `netstat -r`.
`add` ***`NetAddr`*** `mask` ***`NetMask Gateway`***	Aggiunge una nuova route relativa alla rete `NetAddr/NetMask` (es. 10.0.0.0/255.255.255.0) alla routing table, attraverso il next hop `Gateway`.
`delete` ***`NetAddr`*** `mask` ***`NetMask Gateway`***	Aggiunge la route relativa alla rete `NetAddr/NetMask` (es. 10.0.0.0/255.255.255.0), raggiungibile attraverso il next hop `Gateway`, dalla routing table.

ipconfig

- Visualizza e modifica alcuni parametri dello stack IP
- Disponibile solo in Windows
- Sintassi:

```
ipconfig [opzioni]
```

Opzione	Descrizione
`[no param.]`	Visualizza i dati principali della configurazione TCP/IP (indirizzi, netmask, gateway, DNS).
`/all`	Visualizza tutti i dati relativi alla configurazione TCP/IP (indirizzi, netmask, gateway, DNS, tempo di lease DHCP).
`/displaydns`	Visualizza l'attuale cache DNS della macchina.
`/flushdns`	Cancella l'attuale cache DNS della macchina.

Esempio di output (1)

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 130.192.16.81
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:760:400:1:3c71:db18:e713:fd56
        IP Address. . . . . . . . . . . . : 2001:760:400:1:20b:dbff:fe14:50bb
        IP Address. . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
        Default Gateway . . . . . . . . . : 130.192.16.17
                                            fe80::207:ebff:fe7e:c60%8
```

Esempio di output (2)

```
C:\>ipconfig /all

Windows IP Configuration
        Host Name . . . . . . . . . . . . : truciolo
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com 3C920 Fast Ethernet (3C905C-TX)
        Physical Address. . . . . . . . . : 00-0B-DB-14-50-BB
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 130.192.16.81
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:760:400:1:3c71:db18:e713:fd56
        IP Address. . . . . . . . . . . . : 2001:760:400:1:20b:dbff:fe14:50bb
        IP Address. . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
        Default Gateway . . . . . . . . . : 130.192.16.17
                                            fe80::207:ebff:fe7e:c60%8
        DNS Servers . . . . . . . . . . . : 130.192.3.21
                                            130.192.3.24
                                            fec0:0:0:ffff::1%1
                                            fec0:0:0:ffff::2%1
                                            fec0:0:0:ffff::3%1
```

Esempio di output (3)

```
C:\>ipconfig /displaydns

Windows IP Configuration

        www.polito.it
        ----------------------------------------
        Record Name . . . . . : www.polito.it
        Record Type . . . . . : 5
        Time To Live  . . . . : 86398
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        CNAME Record  . . . . : web01.polito.it

        localhost
        ----------------------------------------
        Record Name . . . . . : localhost
        Record Type . . . . . : 1
        Time To Live  . . . . : 0
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        A (Host) Record . . . : 127.0.0.1

        . . .
```

WinDump / tcpdump

- Semplice analizzatore di rete, in forma testuale
  - Molto compatto
  - Visualizza un sommario per ogni pacchetto catturato
  - Il sommario contiene le informazioni più imporanti di ogni protocollo presente nel pacchetto
- Sintassi

```
WinDump [opzioni] [filtro] (Windows)
tcpdump [opzioni] [filtro] (UNIX)
```

- Disponibilità
  - Normalmente incluso di default nelle distribuzioni UNIX
    - `http://www.tcpdump.org/` per la versione più aggiornata
  - Programma a parte in Windows
    - `http://www.winpcap.org/windump/`

WinDump / tcpdump: sintassi

Opzione	Descrizione
`[no param.]`	Visualizza tutto il traffico relativo alla prima interfaccia di rete.
`-D`	Visualizza la lista delle interfacce di rete disponibili.
`-i [numero / interfaccia]`	Cattura il traffico dall'interfaccia specificata, che può essere sia un numero, sia il nome dell'interfaccia stessa. Ambedue i dati sono riportati dall'opzione `-D`.
`-c count`	Cattura `count` pacchetti, al termine del quale il programma esce (default: la cattura viene terminata digitando `Ctrl+C`).
`-r file`	Legge i dati dal file `file`, anzichè catturarli da rete.
`-w file`	Scrive i pacchetti catturati (in forma binaria) sul file `file`. Questi potranno essere richiamati con l'opzione `-r`.
`-n`	Visualizza i pacchetti catturati senza alcuna traduzione di indirizzi / porte dal formato numerico a quello letterale. Aumenta la velocità di esecuzione in quanto non richiede alcuna risoluzione DNS prima della visualizzazione.

WinDump / tcpdump: sintassi di filtraggio (1)

- Definisce quali pacchetti devono essere visualizzati
  - Specifica completa:
    `http://www.winpcap.org/windump/docs/manual.htm`

Filtro	Descrizione
`[nessuno]`	Cattura tutti i pacchetti ricevuti dalla scheda di rete in esame.
`arp`	Cattura solamente pacchetti ARP. Analogamente, è possibile specificare `ip`, `ip6`, `tcp`, `udp`, `icmp`, etc.
`host [host]`	Cattura tutti i pacchetti originati o destinati all'host IP `host`.
`src host [host]`	Cattura tutti i pacchetti originati dall'host IP `host`. Analogamente, `dst host [host]` cattura tutti i pacchetti destinati all'host `host`.

WinDump / tcpdump: sintassi di filtraggio (2)

Filtro	Descrizione
`tcp and port [port]`	Cattura tutti i pacchetti TCP che sono originati o destinati alla porta `port`.
`src port [port]`	Cattura tutti i pacchetti TCP e UDP che hanno il valore `port` come porta sorgente.
`ether host [host]`	Cattura tutti i pacchetti che sono originati o destinati all'host che ha indirizzo MAC pari a `host`. L'indirizzo MAC deve essere nella forma `aa:bb:cc:dd:ee:ff`.
`ether broadcast`	Cattura tutti i pacchetti brodcast a livello MAC.
Operatori booleani: `and, or, not`	E' possibile combinare più espressioni in uno stesso filtro attraverso l'utilizzo degli operatori booleani e delle parentesi (( )) per indicare le precedenze nella valutazione dell'espressione.

Esempio di output

```
C:\>WinDump -n –i eth0
15:35:13.984880 arp who-has 130.192.16.17 tell 130.192.16.81
15:35:13.987947 arp reply 130.192.16.17 is-at 00:e0:1e:ec:3c:84
15:35:13.988058 130.192.16.81 > 192.168.10.2: icmp 40: echo request seq 9984
15:35:13.991419 192.168.10.2 > 130.192.16.81: icmp 40: echo reply seq 9984
15:35:14.979533 130.192.16.81 > 192.168.10.2: icmp 40: echo request seq 10240
15:35:14.982533 192.168.10.2 > 130.192.16.81: icmp 40: echo reply seq 10240
```