Architettura degli Elaboratori 2

Esercitazioni. 6

- analizzatore di protocollo
- sniffer
- utility di rete

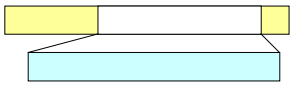
A. Memo - 2005

Pacchetti e imbustamento

- i dati trasmessi sono pacchettizzati (dimensione tipica = 1500 Byte)
- esempio di pacchetto:

```
ff ff ff ff ff ff 00 0e 35 8f d5 7e 08 06 00 01   ........5..~....
08 00 06 04 00 01 00 0e 35 8f d5 7e c0 a8 01 02   ........5..~....
00 00 00 00 00 00 c0 a8 01 01                     ..........
```

intestazione Ethernet
intestazione ARP



Sniffer (1)

- è un programma che permette di catturare interattivamente i pacchetti di dati che percorrono la rete o analizzare quelli già catturati
- configura la scheda in **modalità promiscua**: si considera destinatario di tutti i pacchetti in transito
- non esiste un punto in cui è possibile catturare tutto il traffico

uno sniffer è anche un analizzatore di protocollo

Sniffer (2)

- una funzionalità importante degli sniffer e degli analizzatori di protocollo è la funzione **packet filtering**
- controlla i pacchetti in arrivo e cattura solo quelli che soddisfano alcune condizioni
- vi sono vari metodi per scoprire la presenza di sniffer in rete, il più banale è analizzare la risposta di un PING o di una richiesta ARP ad un indirizzo inesistente, che risponde ! (individuazione modalità promiscua)

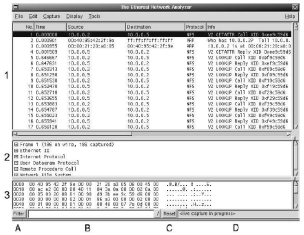
Ethereal (1)

- Ethereal è un analizzatore di protocollo di rete con interfaccia grafica
- permette di catturare interattivamente i pacchetti di dati che percorrono la rete o analizzare quelli già catturati
- esistono altri prodotti:
  - tcpdump (senza interfaccia grafica, Linux)
  - Sniffer Pro della Network Associate

Ethereal (2)

1. pannello Packet List
2. pannello Tree View
3. pannello Data View

A. bottone Filter Editing
B. casella Filter String
C. bottone Reset Filter
D. Information message



Utilizziamo Ethereal per catturare un semplice comando PING

Utility di rete

- ARP
- IPCONFIG
- WINIPCFG
- PING
- file HOSTS
- TRACEROOT e TRACERT
- NETSTAT
- ROUTE
- NET
- TELNET

ARP (1)

gestisce la tabella ARP di sistema:

- cancella o aggiunge una riga della tabella di ARP
- visualizza la tabella di ARP interna

```
C:\>arp -a

Interfaccia: 192.168.0.41 --- 0x2
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.0.40          00-40-d0-67-54-2e     dinamico
  192.168.0.42          00-40-d0-67-54-2f     dinamico
```

ARP (2)

```
C:\>arp -v -a

Visualizza e modifica la tabella di traduzione indirizzo IP-indirizzo fisico
usata dal protocollo di risoluzione (ARP).

ARP -s ind_inet ind_eth [ind_if]
ARP -d ind_inet [ind_if]
ARP -a [ind_inet] [-N ind_if]

 -a            Visualizza le voci ARP correnti prendendole dai dati del
               protocollo. Se viene specificato ind_inet, sono visualizzati
               solo gli indirizzi IP e fisico del computer specificato. Se
               più di un'interfaccia di rete usa ARP, vengono visualizzate
               le voci di ogni tabella ARP.
 -g            Analogo a -a.
 ind_inet      Specifica un indirizzo Internet.
 -N ind_if     Visualizza le voci ARP per l'interfaccia di rete specificata
               da ind_if.
 -d            Elimina l'host specificato da ind_inet. ind_inet può utilizzare
               il carattere jolly per eliminare tutti gli host.
 -s            Aggiunge l'host e associa l'indirizzo Internet ind_inet con
               l'indirizzo fisico ind_eth. L'indirizzo fisico è un numero
               composto da 6 byte esadecimali separati da un trattino.
               La voce è permanente.
 ind_eth       Specifica un indirizzo fisico.
 ind_if        Se presente, specifica l'indirizzo Internet dell'interfaccia
               la cui tabella di traduzione deve essere modificata. Se non
               presente, viene utilizzata la prima interfaccia utilizzabile.

Esempio:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  ....Aggiunge una voce statica.
  > arp -a                                    ....Visualizza la tabella ARP.
```

ARP (3)

Per visualizzare il contenuto di tutta la arp cache, oppure solo l'arp dell'host specificato

arp [opzioni] -a [hostname]

Cancella uno specifico host dall'arp

arp [opzioni] -d hostname

Crea manualmente l'arp di uno specifico host

arp [opzioni] -s hostname hw_addr [opzioni]

Opzioni

-v, --verbose Abilita il verbose mode
-n, --numeric Non esegue il DNS lookup degli indirizzi ip
-H type, --hw-type type, -t type Specifica quale classe di arp deve visualizzare, cancellare o inserire. (ARCnet (arc-net) , PROnet (pronet) , AX.25 (ax25) and NET/ROM (netrom). Default=ether)
-i If, --device If Specifica l'interfaccia
-e Visualizza il risultato in formato standard

Formato pacchetto ARP

0 – 7	8 – 15	16 – 23	24 – 31
Hardware type		Protocol type	
HW size	PR size	Opcode	
Sender MAC Address			
Sender MAC Address		Sender IP Address	
Sender IP Address		Target MAC Address	
Target MAC Address			
Target IP Address			

```
Frame 2 (42 bytes on wire, 42 bytes captured)
    Arrival Time: Mar 12, 2005 18:09:49.041446000
    Time delta from previous packet: 13.872895000 seconds
    Time since reference or first frame: 13.872895000 seconds
    Frame Number: 2
    Packet Length: 42 bytes
    Capture Length: 42 bytes
Ethernet II, Src: 00:0e:35:8f:d5:7e, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (Broadcast)
    Source: 00:0e:35:8f:d5:7e (192.168.1.2)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:0e:35:8f:d5:7e (192.168.1.2)
    Sender IP address: 192.168.1.2 (192.168.1.2)
    Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
    Target IP address: 192.168.1.1 (192.168.1.1)

0000  ff ff ff ff ff ff 00 0e 35 8f d5 7e 08 06 00 01   ........5..~....
0010  08 00 06 04 00 01 00 0e 35 8f d5 7e c0 a8 01 02   ........5..~....
0020  00 00 00 00 00 00 c0 a8 01 01                     ..........
```

IPCONFIG (1)

Serve per vilualizzare i parametri di configurazione di rete.

UTILIZZO: *ipconfig [/? | /all | /renew [scheda] | /release [scheda] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [IDclasse]]*

OPZIONI:		
	/?	*Visualizza questo messaggio*
	/all	*Visualizza le informazioni complete sulla configurazione.*
	/release	*Rilascia l'indirizzo IP per la scheda specificata.*
	/renew	*Rinnova l'indirizzo IP per la scheda specificata.*
	/flushdns	*Svuota la cache del resolver DNS.*
	/registerdns	*Aggiorna tutti i lease DHCP e registra di nuovo i nomi DNS*
	/displaydns	*Visualizza il contenuto della cache del resolver DNS.*
	/showclassid	*Visualizza tutti gli ID classe DHCP consentiti per la scheda.*
	/setclassid	*Modifica l'ID classe DHCP.*

IPCONFIG (2)

L'impostazione predefinita è la visualizzazione soltanto dell'indirizzo IP, dell a *subnet mask* e del *gateway* predefinito per ciascuna scheda associata al TCP/IP.
Per i parametri *Release* e *Renew*, se non è specificato il nome di alcuna scheda, vengono rilasciati o rinnovati i *lease* degli indirizzi IP per tutte le schede associate al TCP/IP.
Per *Setclassid*, se non è specificato alcun *IDclasse*, *l'IDclasse* viene rimosso.

Esempi:

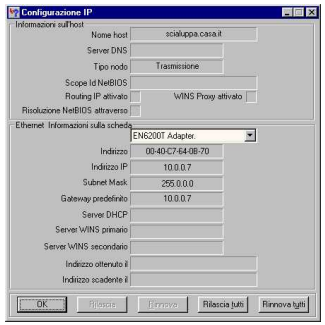
> ipconfig	*... Visualizza informazioni.*
> ipconfig /all	*... Visualizza informazioni dettagliate.*
> ipconfig /renew	*... rinnova tutte le schede*
*> ipconfig /renew EL**	*... rinnova qualsiasi connessione il cui nome inizi per EL*
*> ipconfig /release *Con**	*... rilascia tutte le connessioni corrispondenti, ad es. "Connessione LAN 1" o "Connessione LAN 2"*

IPCONFIG (3)

```
C:\Documents and Settings\Proprietario>ipconfig /all

Configurazione IP di Windows

        Nome host . . . . . . . . . . . . : COMPUTER
        Suffisso DNS primario  . . . . . . :
        Tipo nodo  . . . . . . . . . . . . : Misto
        Routing IP abilitato. . . . . . . . : No
        Proxy WINS abilitato . . . . . . . : No

Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Descrizione . . . . . . . . . . . . : National Semiconductor Corp. DP8
                                              3815/816 10/100 MacPhyter PCI Adapter
        Indirizzo fisico. . . . . . . . . . : 00-03-0D-07-64-BB
        DHCP abilitato. . . . . . . . . . . : No
        Indirizzo IP. . . . . . . . . . . . : 192.168.0.41
        Subnet mask . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . :
```

WINIPCFG

Analogo a ipconfig, per WIN 95/98.



PING (1)

- esegue un controllo di raggiungibilità
- invia un messaggio ICMP *echo request* e si aspetta un *echo reply*
- un host che non risponde è non raggiungibile o l'*echo reply* è disattivata

```
C:\>ping 127.0.0.1

Esecuzione di Ping 127.0.0.1 con 32 byte di dati:

Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128
Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128
Host di destinazione irraggiungibile.

Statistiche Ping per 127.0.0.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  0ms, Medio =  0ms
```

PING (2)

Sintassi: ping [-t] [-a] [-n numero] [-l lunghezza] [-f] [-i TTL] [-v TOS] [-r numero] [-s numero] [[-j elenco-host] | [-k elenco-host]] [-w timeout] elenco-destinazioni

Opzioni:

-t	Esegue Ping sull'host specificato finché non viene interrotto.
-a	Risolve gli indirizzi in nomi host.
-n numero	Invia numero di richieste di eco.
-l lunghezza	Invia dimensione buffer.
-f	Imposta il flag Non frammentare nel pacchetto.
-i TTL	Vita pacchetto.
-v TOS	Tipo di servizio.
-r count	Registra route per il conteggio dei punti di passaggio.
-s count	Marca orario per il conteggio dei punti di passaggio.
-j elenco-host	Instradamento libero lungo l'elenco host.
-k elenco-host	Instradamento ristretto lungo l'elenco host.
-w timeout	Timeout in millisecondi per ogni risposta.

file HOSTS (1)

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Questo è un esempio di file HOSTS usato da Microsoft TCP/IP per Windows.
#
# Questo file contiene la mappatura degli indirizzi IP ai nomi host.
# Ogni voce dovrebbe occupare una singola riga. L'indirizzo IP dovrebbe
# trovarsi nella prima colonna seguito dal nome host corrispondente.
# L'indirizzo e il nome host dovrebbero essere separati da almeno uno spazio
# o punto di tabulazione.
#
# È inoltre possibile inserire commenti (come questi) nelle singole righe
# o dopo il nome del computer caratterizzato da un simbolo '#'.
#
# Per esempio:
#
#      102.54.94.97     rhino.acme.com          # server origine
#       38.25.63.10     x.acme.com              # client host x

127.0.0.1       localhost
```

TRACEROUTE (o TRACERT)

- segue il percorso di un pacchetto, hop per hop
- l'host invia alla porta 33434 del destinatario una sequenza di pacchetti UDP con campo TTL via via crescente
- i vari dispositivi incontrati durante il percorso risponderanno con il messaggio
  - *Time Exceeded* (i router)
  - *Port Unreachable* (il destinatario)

```
C:\>tracert

Sintassi: tracert [-d] [-h max_salti] [-j elenco-host] [-w timeout] nome_destinazione

Opzioni:
    -d                  Non risolve gli indirizzi in nome host.
    -h max_salti        Numero massimo di punti di passaggio per ricercare la destinazione.
    -j elenco-host      Instradamento libero lungo l'elenco host.
    -w timeout          Timeout in millisecondi per ogni risposta.
```

TRACERT

```
C:\WINDOWS>tracert volftp.tin.it

Rilevazione instradamento verso cam.ca.tin.it [195.31.191.10]
su un massimo di 30 punti di passaggio:

  1  1787 ms  2211 ms  1721 ms  pppsrv05.stm.it [195.62.32.50]
  2  2610 ms  1326 ms  1348 ms  world.stm.it [195.62.32.11]
  3  3098 ms  2099 ms  1729 ms  eth0-ibs-gw.stm.it [195.62.34.2]
  4  1976 ms  3040 ms  2394 ms  r-rm2-torreargentina.interbusiness.it [151.99.9.181]
  5     *        *        *     Richiesta scaduta.
  6     *        *        *     Richiesta scaduta.
  7  2555 ms  1736 ms  3118 ms  r-mi5-rm5-atm.interbusiness.it [151.99.101.1]
  8     *        *     3029 ms  r-mi6-fa2.interbusiness.it [151.99.100.37]
  9  2221 ms  2606 ms     *     r-tin-mi6-atm.interbusiness.it [151.99.107.134]
 10     *        *        *     Richiesta scaduta.
 11     *        *        *     Richiesta scaduta.
 12     *        *     1753 ms  cam.ca.tin.it [195.31.191.10]

Rilevazione completata.
```

NETSTAT (1)

permette di visualizzare:

- le connessioni di rete e l'elenco dei socket attivi
- le tabelle di routing *(-route)*
- le statistiche di traffico delle singole interfacce *(-interface)*
- le statistiche per ciascun protocollo *(-statistics)*
- connessioni mascherate *(-masquerade)*
- i membri di gruppi multicast *(-groups)*

NETSTAT (1)

netstat [information-type] [options]

Information Type
--route , -r Visualizza le route impostate sul sistema
--groups , -g Visualizza informazioni riguardanti i multicast group membership (ipv4 e ipv6)
--interface=iface , -i Visualizza le statistiche di tutte le interfacce o della singola interfaccia specificata
--masquerade , -M Verifica le connessioni che hanno subito masquerading
--statistics , -s Visualizza un sommario di statistiche

Options
--verbose , -v Abilita il verbose mode.
--numeric , -n Non risolve gli Ip e il numero delle porte, risparmiando i tempi per query DNS.
--protocol=family , -A Opzione per specificare l'address family quando si vuole visualizzare le connessioni.
-c, --continuous Esegue il comando ogni secondo (o ogni intervallo di secondi specificato).
-p, --program Mostra il PID, ed il nome del programma proprietario della socket. Utile per capire, per esempio, quale programma utilizza una specifica porta TCP.
-l, --listening Mostra solo le connessioni in LISTENING
-a, --all Mostra tutte le connessioni (LISTENING e non), se abbinato al flag -i visualizza le informazioni per tutte le interfacce

NETSTAT (2)

```
C:\WINDOWS>netstat /?

Visualizza statistiche su protocollo e connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervallo]

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -e            Visualizza le statistiche Ethernet. L'opzione può essere
                associata all'opzione -s.
  -n            Visualizza gli indirizzi e i numeri di porta in forma numerica.
  -p proto      Visualizza connessioni del protocollo specificato da 'proto';
                'proto' può essere TCP o UDP. Se usato con l'opzione -s per le
                statistiche, 'proto' può essere TCP, UDP, o IP.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo. Per impostazione
                predefinita, le statistiche sono visualizzate per TCP, UDP
                e IP; l'opzione -p può essere utilizzata per specificare
                un sottoinsieme dell'impostazione predefinita.
  intervallo    Rivisualizza le statistiche selezionate, interrompendo
                per un numero di secondi pari a "intervallo" tra ogni
                visualizzazione. Premere Control-C per fermare la visualizzazione
                delle statistiche. Se omesso, netstat stamperà le informazioni
                di configurazione correnti una sola volta.
```

NETSTAT (3)

```
C:\WINDOWS>netstat -na

Connessioni attive

  Proto  Indirizzo locale         Indirizzo remoto           Stato
  TCP    0.0.0.0:0                0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1026             0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1028             0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1035             0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1036             0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1037             0.0.0.0:0                  LISTENING
  TCP    0.0.0.0:1038             0.0.0.0:0                  LISTENING
  TCP    195.62.37.17:1026        195.62.32.254:119          ESTABLISHED
  TCP    195.62.37.17:1028        195.62.32.254:119          ESTABLISHED
  TCP    195.62.37.17:1035        194.133.0.17:80            CLOSE_WAIT
  TCP    195.62.37.17:1036        194.133.0.17:80            CLOSE_WAIT
  TCP    195.62.37.17:1037        194.133.0.17:80            CLOSE_WAIT
  TCP    195.62.37.17:1038        194.133.0.17:80            CLOSE_WAIT
```

NETSTAT (4)

```
C:\WINDOWS>netstat -es
Statistiche interfaccia

                           Ricevuti            Trasmessi

Byte                        349919              56810
Pacchetti unicast              881                769
Pacchetti non-unicast           10                 10
Scarto                           0                  0
Errori                           0                  0
Protocolli sconosciuti          23

Statistiche IP

  Pacchetti ricevuti            = 882
  Errori di intestazione ricevuti = 0
  Errori di indirizzo ricevuti  = 5
  .....
Statistiche ICMP  ......
Statistiche TCP   ......
Statistiche UDP   ......
```

NETSTAT (5)

```
C:\WINDOWS>netstat -r

Tabella di Route

Route attive:

  Indirizzo rete           Maschera Indirizzo gateway      Interfac.  Metric
          0.0.0.0          0.0.0.0      195.62.38.6      195.62.38.6       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
      195.62.38.0    255.255.255.0      195.62.38.6      195.62.38.6       1
      195.62.38.6  255.255.255.255        127.0.0.1        127.0.0.1       1
    195.62.38.255  255.255.255.255      195.62.38.6      195.62.38.6       1
        224.0.0.0        224.0.0.0      195.62.38.6      195.62.38.6       1
  255.255.255.255  255.255.255.255      195.62.38.6      195.62.38.6       1

Connessioni attive

  Proto  Indirizzo locale         Indirizzo remoto           Stato
  TCP    bejor:1026               news.stm.it:nntp       ESTABLISHED
  TCP    bejor:1028               news.stm.it:nntp       ESTABLISHED
```

ROUTE (1)

Route permette di manipolare le tabelle di routing, aggiungendo ed eliminando route statiche e default gateway, e di visualizzare la tabella di routing di un sistema.

route add [-net|-host] indirizzo [gw *gateway*] [netmask *netmask*] [mss *mss*] [metric *metric*] [dev *device*]

route del *indirizzo*

Per aggiungere una route statica per un'intera rete si usa l'opzione add e si definisce la rete con -net. Per esempio:
route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.0.254
Aggiunge una route statica per la rete 192.168.0.0/24 usando come gateway 10.0.0.254.

ROUTE (2)

Per impostare il default gateway si può digitare qualcosa come:
route add -net 0.0.0.0 netmask 0.0.0.0 gw 10.0.0.1 oppure:
route add default gw 10.0.0.1

Per cancellare una route esistente basta indicare il nome della rete:
route del -net 192.168.0.0

Per visualizzare la tabella di route basta: **route**, se si vuole evitare il reverse lookup degli IP e velocizzare l'operazione scrivere: **route -n**

Per visualizzare la cache del sistema sulle route usate: **route -C**

ROUTE (3)

```
C:\Documents and Settings\Proprietario>route

Modifica le tabelle di routing della rete.

ROUTE [-f] [-p] [comando [destinazione]
                [MASK netmask] [gateway] [METRIC passi] [interfaccia IF]

  -f            Cancella le tabelle di routing di tutte le voci gateway.
                Se usato insieme ad uno dei comandi, le tabelle
                vengono cancellate prima dell'esecuzione del comando.

  -p            Quando si usa con il comando ADD, mantiene una route
                ad ogni avvio del sistema. Normalmente, invece, le route non
                sono conservate quando si riavvia il sistema. Usato insieme al
                comando PRINT, mostra l'elenco delle route permanenti
                registrate. Viene ignorato da tutti gli altri comandi, che
                modificano sempre le route permanenti appropriate.
                Opzione non supportata da Windows 95.
  comando       Specifica uno dei quattro comandi:
                 PRINT     Stampa una route
                 ADD       Aggiunge una route
                 DELETE    Elimina una route
                 CHANGE    Modifica una route esistente
  destinazione  Specifica l'host.
  MASK          Se MASK viene specificato, l'argomento successivo viene
                interpretato come la maschera di rete.
  netmask       Specifica un valore maschera per la subnet da associare
                alla voce di route. Se non specificato viene assunto
                255.255.255.255.
  gateway       Specifica il gateway.
  interfaccia   Numero di interfaccia er la route specificata.
  METRIC        Specifica i passi/costo per la destinazione
```

ROUTE (4)

```
Tutti i nomi simbolici utilizzati come destinazione sono risolti nel file di
database NETWORKS. I nomi simbolici per il gateway sono risolti nel file di
database dei nomi di host HOSTS.

Se il comando è PRINT o DELETE, è possibile usare caratteri jolly
(i caratteri jolly sono specificati come "*") in destinazione o gateway,
o omettere l'argomento gateway.

Se Dest contiene * o ?, è considerato come un modello di shell e
sono stampate solo le route di destinazione corrispondenti. La "*" corrisponde
a una stringa qualsiasi e "?" corrisponde a un qualsiasi carattere.
Esempi: 157.*.1, 157.*, 127.*, *224*.
Note di diagnostica:
    MASK non valido genera un errore quando (DEST & MASK) != DEST.
    Esempio> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             L'aggiunta della route non è riuscita: il parametro mask specificato
             non è valido. (Destinatione e Mask) != Destinazione.

Esempi:

    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destinazione^      ^mask      ^gateway     metric^    ^
                                                          Interfaccia^
      Se IF non è data, viene cercata la migliore interfaccia per un dato gateway
    > route PRINT
    > route PRINT 157*          .... Stampa solo route corrispondenti 157*
    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE è utilizzato solo per modificare gateway e/o metric.
    > route PRINT
    > routeDELETE 157.0.0.0
    > route PRINT
```