Traffic monitoring και παρουσίαση ενός router

8ο Φροντιστήριο

ΗΥ 335

Εισαγωγή στο tcpdump

- Εργαλείο για την παρακολούθηση δικτυακής κίνησης
- Χρησιμοποιείται για την συλλογή και προβολή πακέτων που εκπέμπονται ή λαμβάνονται σε ένα δίκτυο
- Χρήση φίλτρων για απομόνωση των πληροφοριών που έχουν ενδιαφέρον

Σύνταξη

- tcpdump [options] [filter expression]
- Παρουσιάζει τα πακέτα που ικανοποιούν τη συνθήκη-φίλτρο με τη μορφή που καθορίζουν οι επιλογές
- man tcpdump για περισσότερες πληροφορίες
- Τρέχει με root δικαιώματα:
  - `$sudo tcpdump` (Debian based)

Παράδειγμα επιλογών

- Παρακολούθηση πακέτων που στέλνονται/λαμβάνονται από το interface wlan0:
  - tcpdump –i eth0
- Αποθήκευση των πακέτων που πιάνονται, σε ένα αρχείο:
  - tcpdump –w <filename>
- Αποθήκευση ολόκληρου του πακέτου:
  - tcpdump –s 0
- Εκτύπωση του πακέτου σε ASCII:
  - tcpdump –A
- Μη μετάφραση των host adresses σε names:
  - tcpdump –n

Παράδειγμα φίλτρων

- Μόνο τα udp πακέτα:
  - tcpdump “udp”
- Μόνο DNS requests (destination port 53):
  - tcpdump “udp dst port 53”
- Μόνο DNS replies (source port 53):
  - tcpdump “udp src port 53”
- Μόνο τα πακέτα προς το mail.google.com:
  - tcpdump “dst host mail.google.com”
- Μόνο τα πακέτα από το mail.google.com:
  - tcpdump “src host mail.google.com”

tcpdump : DNS request&reply

```
$ tcpdump -i wlan0 -n udp
15:47:52.321429 IP
   192.168.1.10.43694 >
   195.170.0.1.53: 51337+ A?
   http://www.csd.uoc.gr. (32)
15:47:52.418720 IP
   195.170.0.1.53 >
   192.168.1.10.43694: 51337
   2/2/2 CNAME ixion.csd.uoc.gr.,
   (138)
```

request

reply

timestamp

src IP

src port

dest port

dest IP

payload size

Εργαλεία με γραφική διεπαφή

- Το wireshark είναι ένα multi-platform εργαλείο που λειτουργεί παρόμοια με το tcpdump, με γραφικό περιβάλλον
- Διαθέσιμο στο www.wireshark.org

DNS request/reply

- DNS request: Ζητάμε από έναν DNS server να μας μεταφράσει ένα host name σε IP address
- Είναι udp πακέτο και ο DNS server «ακούει» στην port 53
- Η DNS reply είναι πάλι ένα udp πακέτο που στέλνει ο DNS στον host μας, στην port 53
- Όταν ανοίξουμε έναν browser και γράψουμε το όνομα ενός site, ο host μας θα στείλει DNS request σε έναν DNS server προκειμένου να μάθει την IP του site στο οποίο θέλουμε να συνδεθούμε

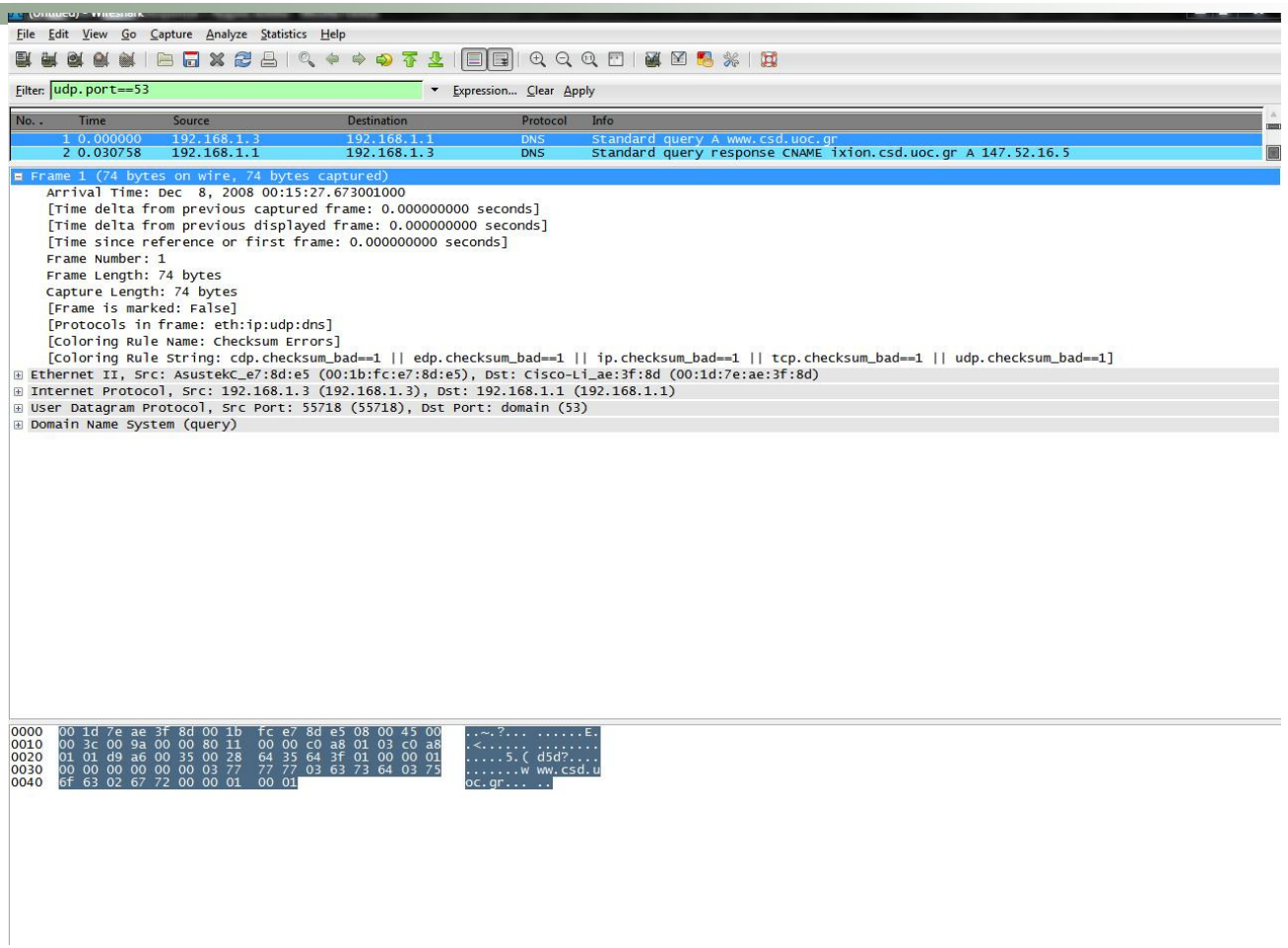
How to capture packets with wireshark

- Επιλέγουμε το interface που θέλουμε να παρακολουθήσουμε από το πρώτο από αριστερά εικονίδιο και πατάμε “start”
- Επιλέγουμε μια συνθήκη-φίλτρο, για να πιάσουμε τα πακέτα που μας ενδιαφέρουν και πατάμε “apply” για να εφαρμοστεί
  - Είτε γράφουμε μια στο textbox δεξιά από το “filter:”
  - Είτε επιλέγουμε μια έτοιμη συνθήκη από το κουμπί “expressions”
- Δημιουργούμε traffic
  - π.χ ανοίγουμε το www.csd.uoc.gr με έναν browser

Display packets with wireshark

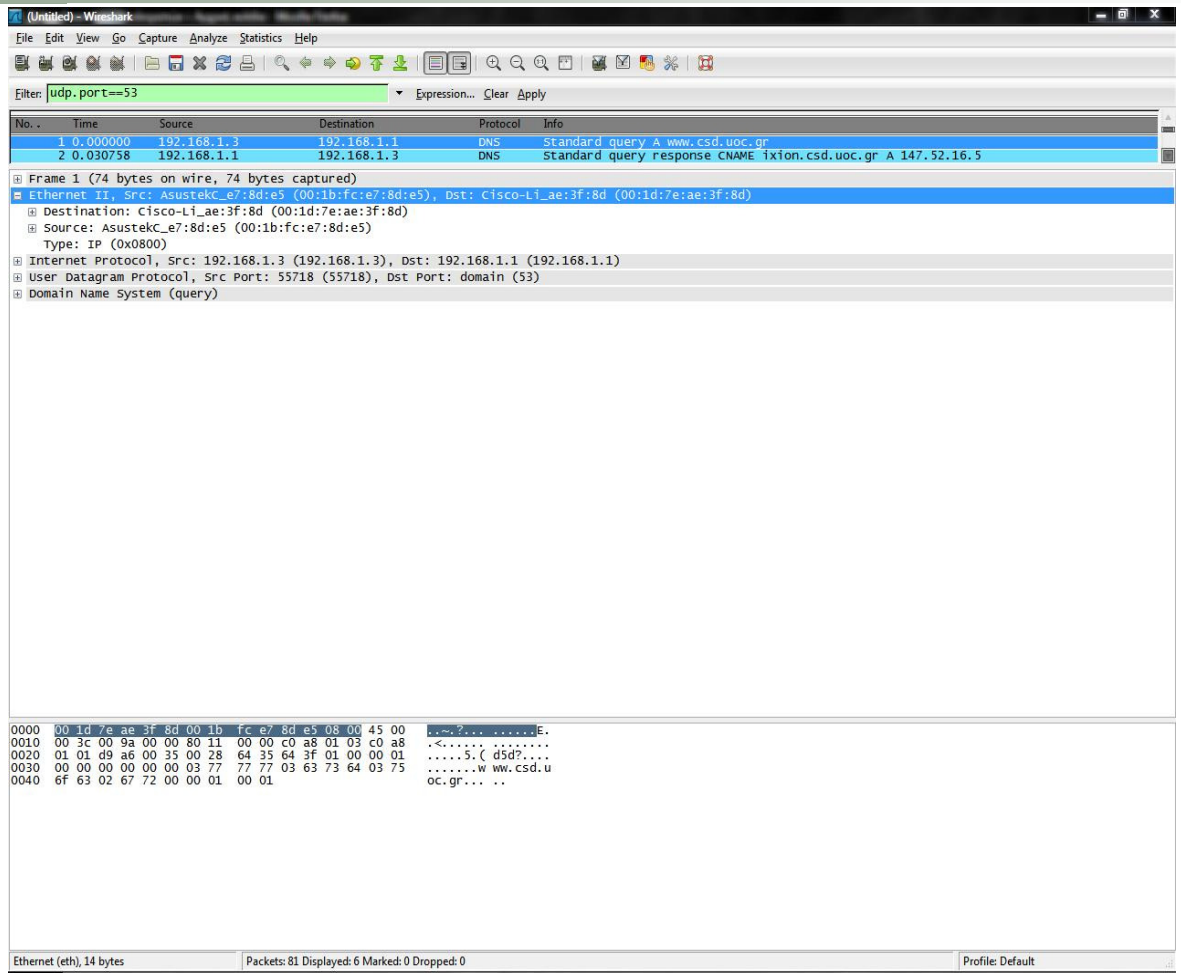
- Το πάνω παράθυρο περιλαμβάνει όλα τα captured πακέτα και μπορούμε να επιλέξουμε κάποιο
- Το μεσαίο παράθυρο δείχνει τα στοιχεία για το πακέτο που είναι επιλεγμένο από τα κάτω επίπεδα προς τα πάνω
  - Από ethernet frame, σε IP segment, UDP datagram και τέλος το payload
- Το κάτω παράθυρο είναι το πακέτο σε hex και μια μετάφραση του σε ASCII
  - Μπορούμε να διαβάσουμε το payload του πακέτου

Capturing DNS traffic

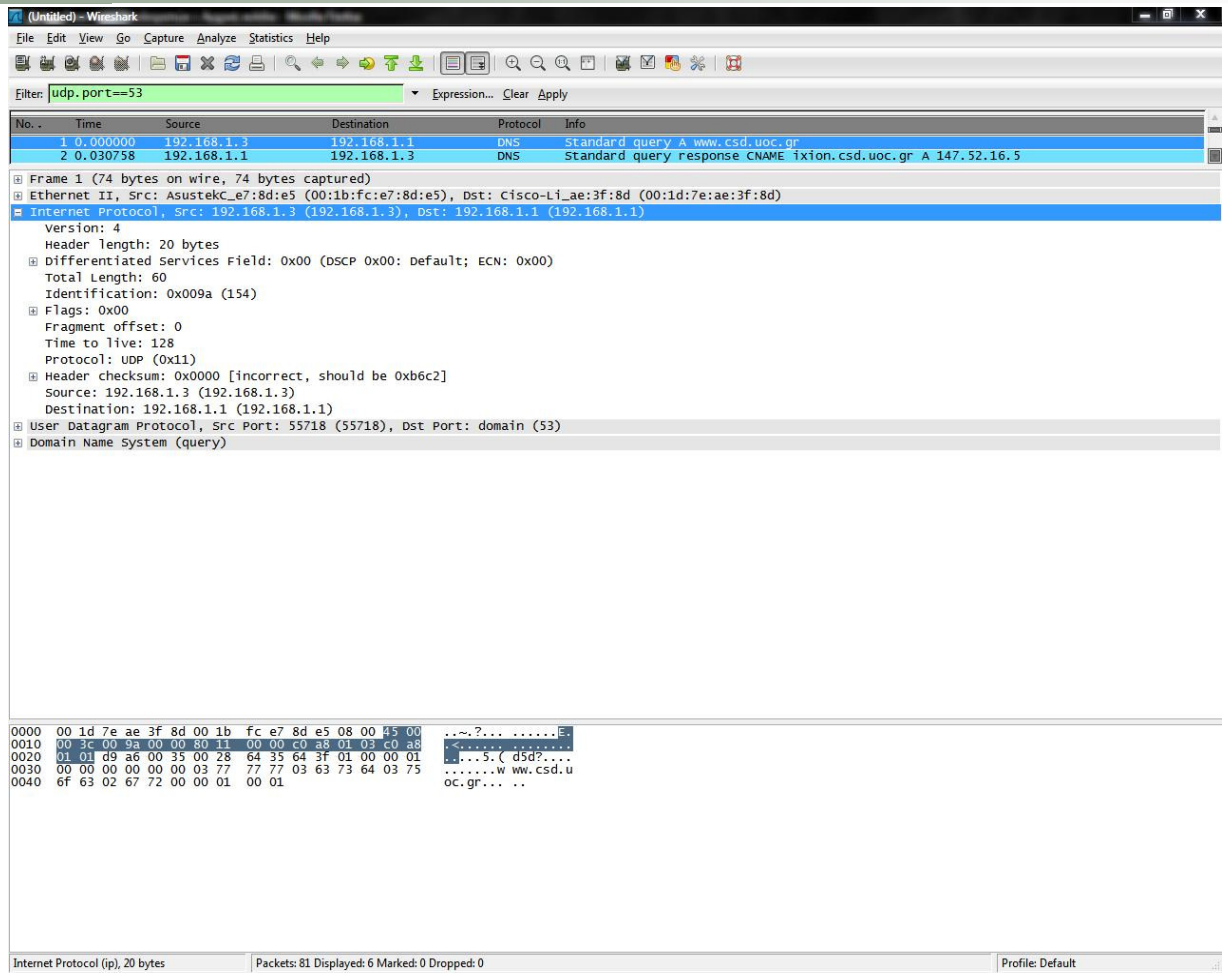


filter:udp.port==53, to capture dns traffic

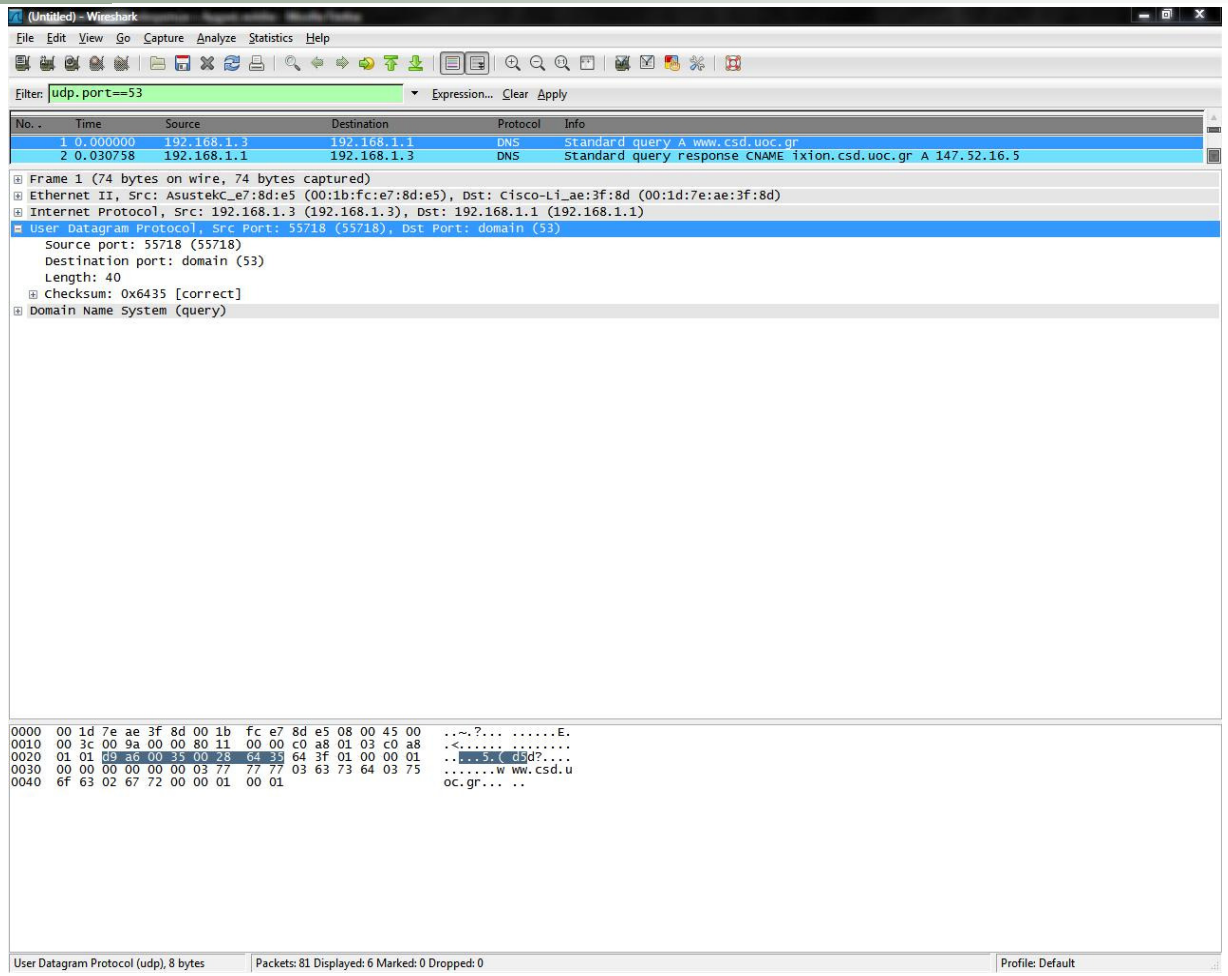
Link layer – ethernet frame



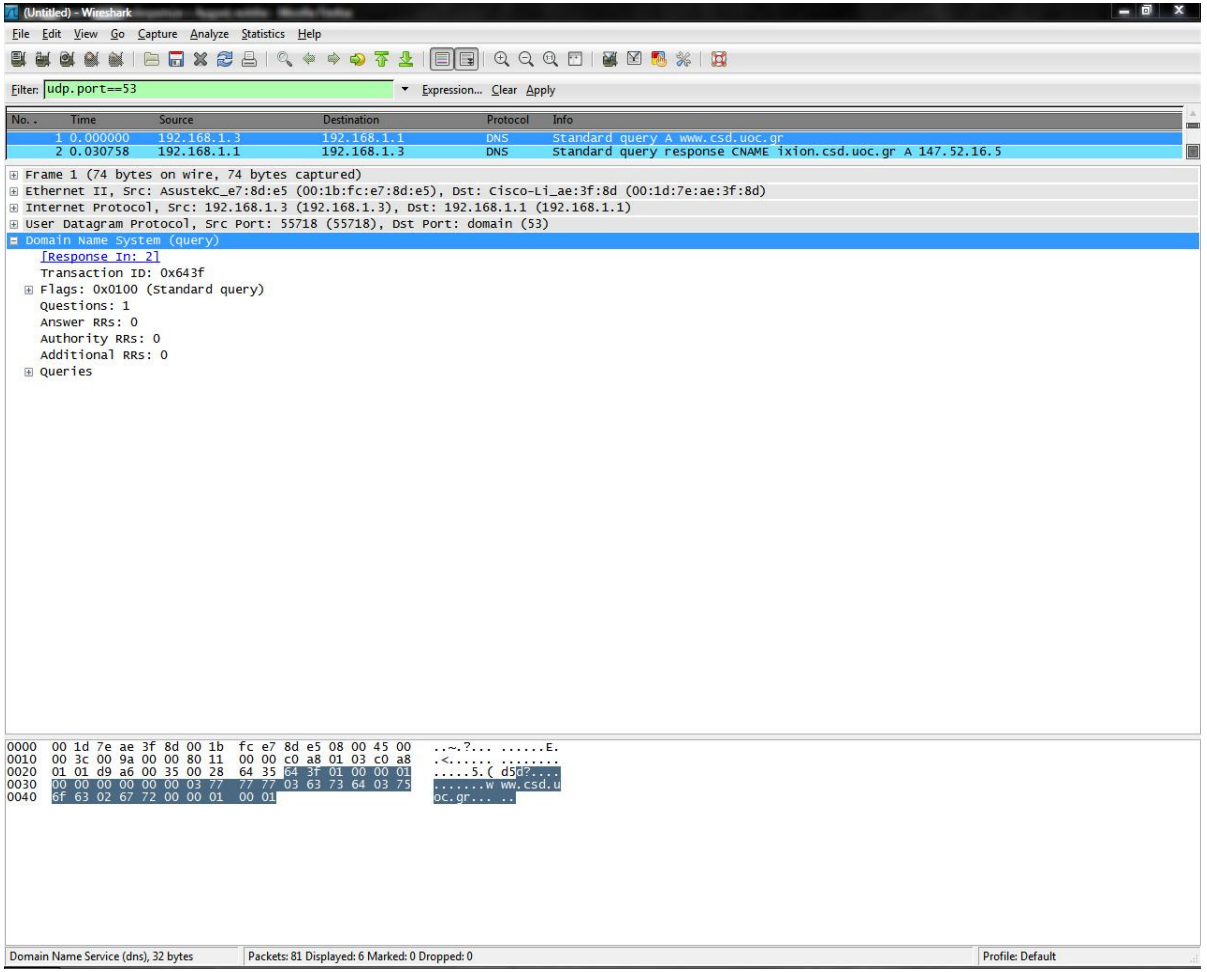
Network layer – IP segment



Transport layer – UDP datagram



Application layer – DNS query



Bonus router!

- Cisco 7200 router
- Show routing table
- Show interface parameters
- Show flow statistics

Show routing table

```
comrt#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2       E1
       - OSPF external type 1, E2 - OSPF external type 2, E - EGP       i -
       IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR       P -
       periodic downloaded static route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
     147.52.0.0/16 is variably subnetted, 4 subnets, 3 masks
C    147.52.20.128/25 is directly connected, FastEthernet2/1
C    147.52.20.0/25 is directly connected, ATM1/0.1
C    147.52.17.0/24 is directly connected, FastEthernet2/0
C    147.52.1.88/30 is directly connected, ATM1/0.3
     10.0.0.0/24 is subnetted, 1 subnets
S    10.10.12.0 [1/0] via 139.91.182.208
     192.168.1.0/32 is subnetted, 1 subnets
C    192.168.1.48 is directly connected, Loopback10
S*   0.0.0.0/0 is directly connected, FastEthernet2/0
```

Show interface parameters

```
comrt#show interface FastEthernet2/0
FastEthernet2/0 is up, line protocol is up
Hardware is AmdFE, address is 0050.73d3.dd38 (bia 0050.73d3.dd38)
Internet address is 147.52.17.85/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX  ARP type: ARPA, ARP
Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 1 drops
5 minute input rate 3000 bits/sec, 5 packets/sec  5 minute output rate 1000 bits/sec, 1
      packets/sec     78251 packets input, 6859600 bytes
      Received 59752 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog
      0 input packets with dribble condition detected
      6197 packets output, 630385 bytes, 0 underruns(0/0/0)
      0 output errors, 0 collisions, 4 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
```

Show flow statistics

```
comrt#sh ip cache flow
IP packet size distribution (31916 total packets):
   1-32   64   96  128  160  192  224  256
    288  320  352  384  416  448  480
   .001 .769 .045 .000 .000 .008 .022 .027 .003 .002
   .000 .000 .042 .000 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096
   4608
   .000 .000 .000 .075 .000 .000 .000 .000 .000 .000
   .000
```

Show flow statistics (cont'd)

```
IP Flow Switching Cache, 4456704 bytes
       11 active, 65525 inactive, 14948 added
       258732 ager polls, 0 flow alloc failures
       Active flows timeout in 30 minutes
       Inactive flows timeout in 15 seconds
       last clearing of statistics neverProtocol
       Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
       --------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
       TCP-Telnet          30      0.0       131    41      0.1      22.5      15.1
       TCP-FTP              2      0.0         1    48      0.0       1.5      15.9
       TCP-WWW            607      0.0         1    42      0.0       0.4       7.8
       TCP-X               85      0.0         1    40      0.0       0.0      15.0
       TCP-other          735      0.0         2    52      0.0       2.9      14.6
       UDP-other         5090      0.1         1   358      0.1       0.4      15.4
       ICMP              8388      0.2         1    57      0.4       1.5      15.4
       Total:           14937      0.4         1   124      0.8       1.2      15.1

       SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  PktsFa2/0         147.52.17.169   Local
       147.52.17.85    01 0000 0800     1
       Fa2/0         147.52.17.169
       Fa2/1         147.52.20.141   01 0000 0800     1
       Fa2/0         147.52.17.169   Null          147.52.20.140   01 0000 0800     4
       Fa2/0         147.52.17.169   Null          147.52.20.137   01 0000 0800     3
       Fa2/0         147.52.17.169   Null          147.52.20.136   01 0000 0800     3
       Fa2/0         147.52.17.169   Null          147.52.20.139   01 0000 0800     5
       Fa2/0         147.52.17.169   Null          147.52.20.133   01 0000 0800     5
       Fa2/0         147.52.17.169   Null          147.52.20.135   01 0000 0800     5
       Fa2/0         147.52.17.169   Null          147.52.20.134   01 0000 0800     3
       Fa2/0         147.52.17.169   AT1/0.1       147.52.20.12    01 0000 0800     2
       Fa2/0         79.131.124.190  Local         147.52.20.11    06 C1D7 0017    25
```

The End