ICMP and SNMP

Foundations of computer networks

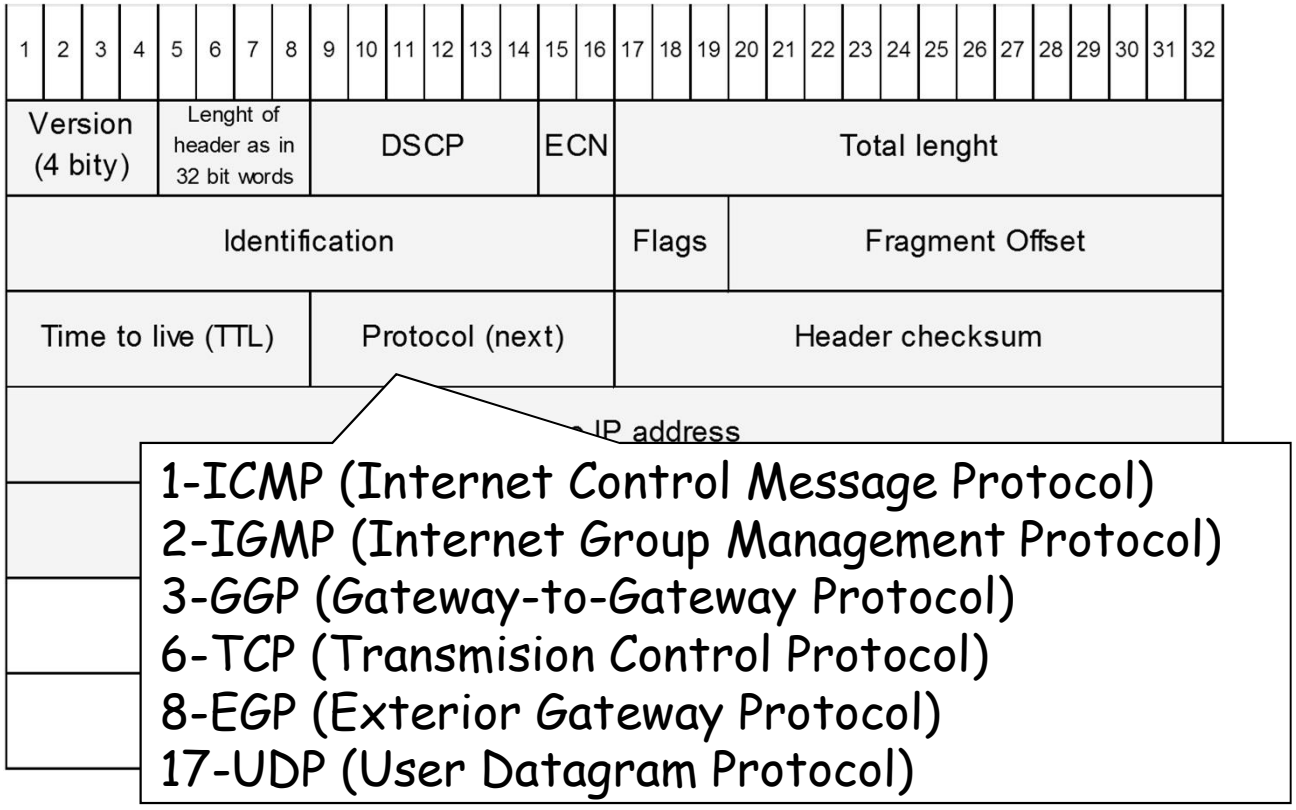
Internet Control Message Protocol

- messages about error
- echo request
- echo response
- flow control
- time control

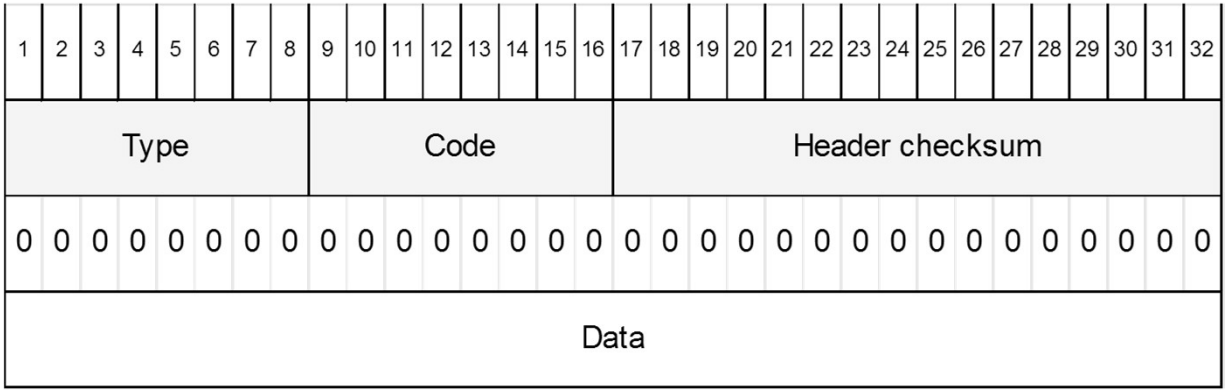
ICMP – main features

- connectionless protocol
- no confirmation (acknowledges)
- no ICMP about ICMP
- in the case of IP fragmentation, ICMP only for first part with error
- no ICMP for broadcast and multicast transmission

IPv4


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
Version (4 bity)
Lenght of header as in 32 bit words
DSCP
ECN
Total lenght
Identification
Flags
Fragment Offset
Time to live (TTL)
Protocol (next)
Header checksum
IP address
1-ICMP (Internet Control Message Protocol)
2-IGMP (Internet Group Management Protocol)
3-GGP (Gateway-to-Gateway Protocol)
6-TCP (Transmision Control Protocol)
8-EGP (Exterior Gateway Protocol)
17-UDP (User Datagram Protocol)

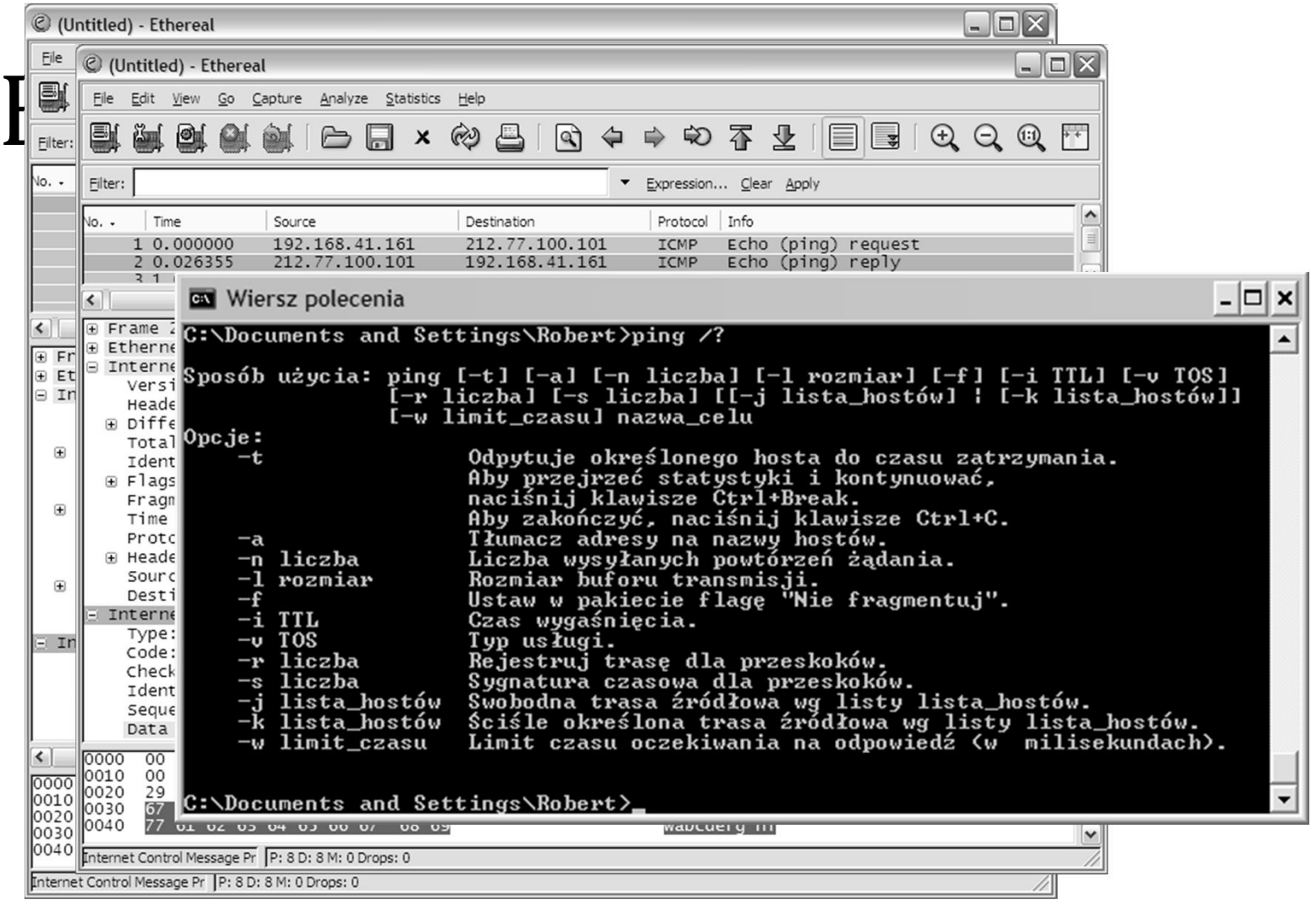
Format ICMP

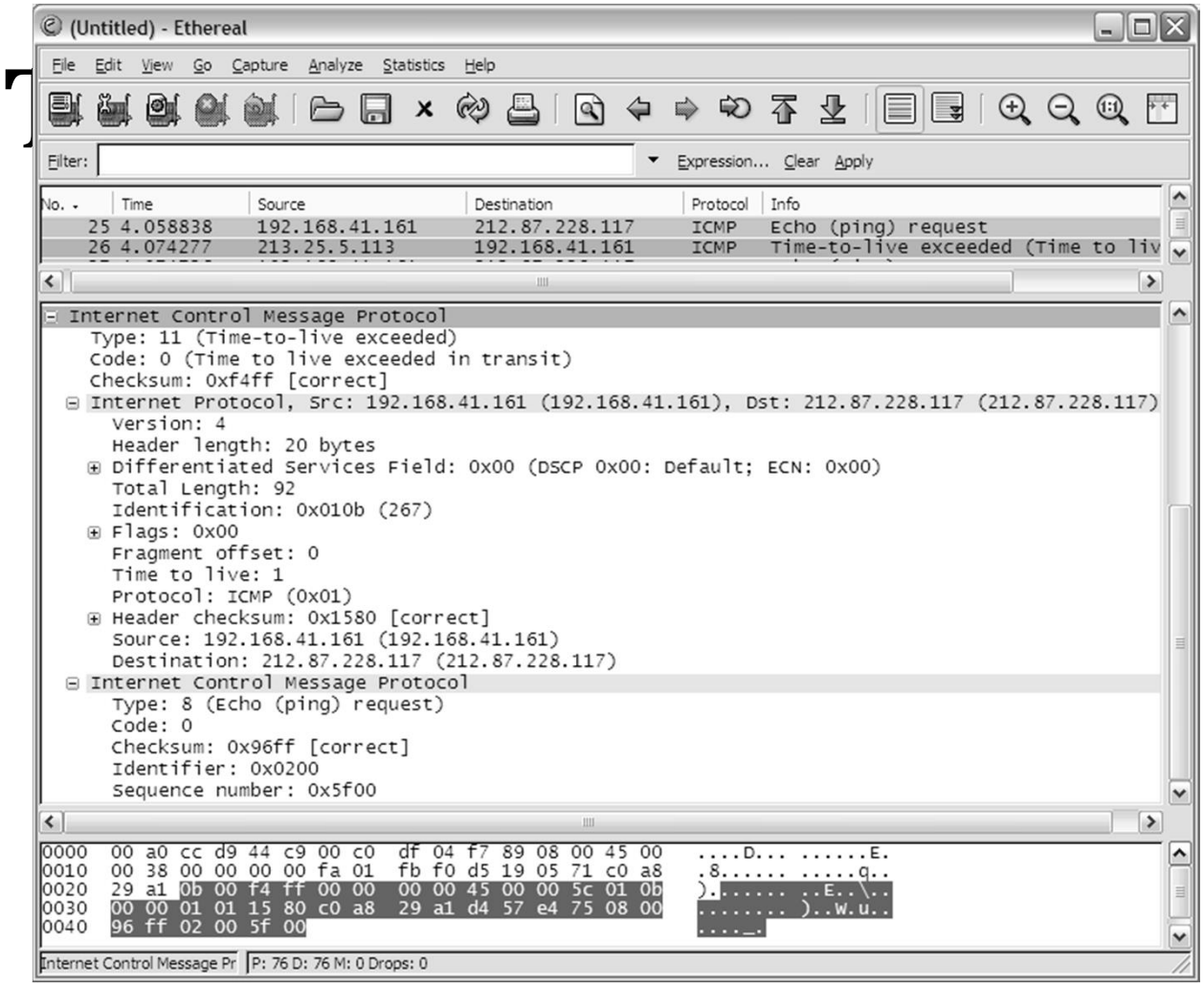

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
Type
Code
Header checksum
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Data

ICMP types and codes

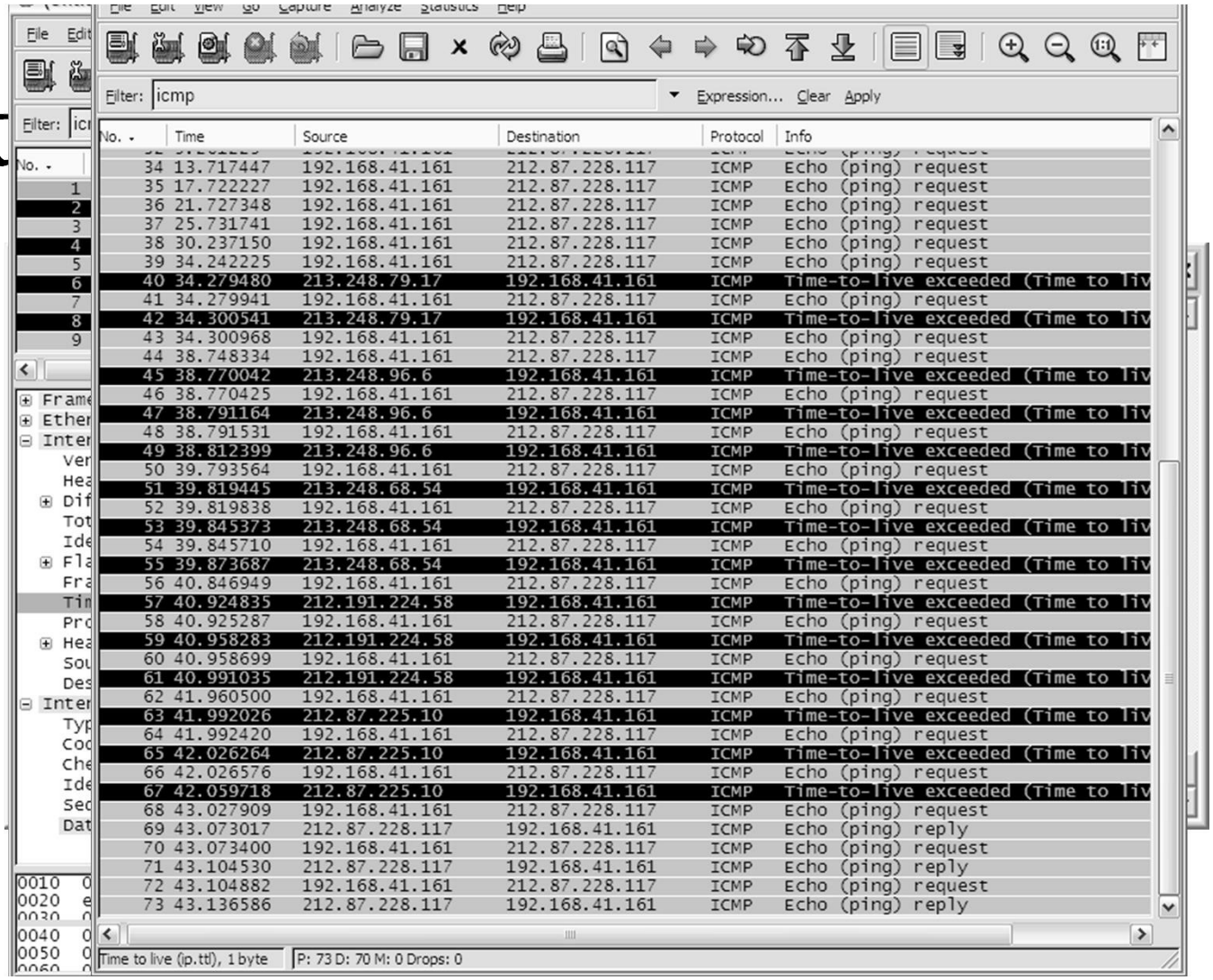
Type	Code	Description
0	0	**Echo replay**
3		**Destination unreachable**
	0	network unreachable
	1	host unreachable
	2	prtocol unreachable
	3	port unreachable
	4	fragmentation required but forbidden
	5	source route failed
	6	network unknown
	7	host unknown
	8	host isolated (absolete)
	9	network prohibited (by administator)
	10	host prohibited (by administrator)
	11	network unreachable for TOS
	12	host unreachable for TOS
	13	communication prohibited by administrator
	14	host precedence violation
	15	shut down in progress
4	0	**Bufers or queue full (absolete)**

Type	Code	Description
5		**Redirect request**
	0	for the network
	1	for teh host
	2	for the network fot TOS
	3	for the host for TOS
8	0	**Echo request**
9	0	**Router advertisement**
10	0	**Router discovery/selection/solicitation**
11		**TTL expired**
	0	in transit
	1	in defragmentation (one of fragment)
12		**Bad IP header**
	0	varius problems
	1	missing options but required
	1	bad length
13	0	**Timestamp request**
14	0	**Timestamp replay**
15	0	**Information request (absolete)**
16	0	**Information replay (absolete)**
17	0	**Address mask request**
18	0	**Address mask replay**


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.41.161 212.77.100.101 ICMP Echo (ping) request
2 0.026355 212.77.100.101 192.168.41.161 ICMP Echo (ping) reply
Wiersz polecenia
C:\Documents and Settings\Robert>ping /?
Sposób użycia: ping [-t] [-a] [-n liczba] [-l rozmiar] [-f] [-i TTL] [-v TOS]
[-r liczba] [-s liczba] [[-j lista_hostów] | [-k lista_hostów]]
[-w limit_czasu] nazwa_celu
Opcje:
-t Odpytuje określonego hosta do czasu zatrzymania.
Aby przejrzeć statystyki i kontynuować,
naciśnij klawisze Ctrl+Break.
Aby zakończyć, naciśnij klawisze Ctrl+C.
-a Tłumacz adresy na nazwy hostów.
-n liczba Liczba wysyłanych powtórzeń żądania.
-l rozmiar Rozmiar buforu transmisji.
-f Ustaw w pakiecie flagę "Nie fragmentuj".
-i TTL Czas wygaśnięcia.
-v TOS Typ usługi.
-r liczba Rejestruj trasę dla przeskoków.
-s liczba Sygnatura czasowa dla przeskoków.
-j lista_hostów Swobodna trasa źródłowa wg listy lista_hostów.
-k lista_hostów Ściśle określona trasa źródłowa wg listy lista_hostów.
-w limit_czasu Limit czasu oczekiwania na odpowiedź (w milisekundach).
C:\Documents and Settings\Robert>
Internet Control Message Pr
P: 8 D: 8 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
25 4.058838 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
26 4.074277 213.25.5.113 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
Internet Protocol, Src: 192.168.41.161 (192.168.41.161), Dst: 212.87.228.117 (212.87.228.117)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 92
Identification: 0x010b (267)
Flags: 0x00
Fragment offset: 0
Time to live: 1
Protocol: ICMP (0x01)
Header checksum: 0x1580 [correct]
Source: 192.168.41.161 (192.168.41.161)
Destination: 212.87.228.117 (212.87.228.117)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x96ff [correct]
Identifier: 0x0200
Sequence number: 0x5f00
0000 00 a0 cc d9 44 c9 00 c0 df 04 f7 89 08 00 45 00 ....D... ......E.
0010 00 38 00 00 00 00 fa 01 fb f0 d5 19 05 71 c0 a8 .8...... .....q..
0020 29 a1 0b 00 f4 ff 00 00 00 00 45 00 00 5c 01 0b).....E..\..
0030 00 00 01 01 15 80 c0 a8 29 a1 d4 57 e4 75 08 00 .....)..W.u..
0040 96 ff 02 00 5f 00 ....
Internet Control Message Pr
P: 76 D: 76 M: 0 Drops: 0

t


File Edit View Go Capture Analyze Statistics Help
Filter: icmp
Expression... Clear Apply
No. Time Source Destination Protocol Info
34 13.717447 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
35 17.722227 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
36 21.727348 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
37 25.731741 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
38 30.237150 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
39 34.242225 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
40 34.279480 213.248.79.17 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
41 34.279941 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
42 34.300541 213.248.79.17 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
43 34.300968 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
44 38.748334 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
45 38.770042 213.248.96.6 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
46 38.770425 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
47 38.791164 213.248.96.6 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
48 38.791531 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
49 38.812399 213.248.96.6 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
50 39.793564 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
51 39.819445 213.248.68.54 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
52 39.819838 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
53 39.845373 213.248.68.54 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
54 39.845710 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
55 39.873687 213.248.68.54 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
56 40.846949 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
57 40.924835 212.191.224.58 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
58 40.925287 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
59 40.958283 212.191.224.58 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
60 40.958699 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
61 40.991035 212.191.224.58 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
62 41.960500 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
63 41.992026 212.87.225.10 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
64 41.992420 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
65 42.026264 212.87.225.10 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
66 42.026576 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
67 42.059718 212.87.225.10 192.168.41.161 ICMP Time-to-live exceeded (Time to liv
68 43.027909 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
69 43.073017 212.87.228.117 192.168.41.161 ICMP Echo (ping) reply
70 43.073400 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
71 43.104530 212.87.228.117 192.168.41.161 ICMP Echo (ping) reply
72 43.104882 192.168.41.161 212.87.228.117 ICMP Echo (ping) request
73 43.136586 212.87.228.117 192.168.41.161 ICMP Echo (ping) reply
Time to live (ip.ttl), 1 byte
P: 73 D: 70 M: 0 Drops: 0

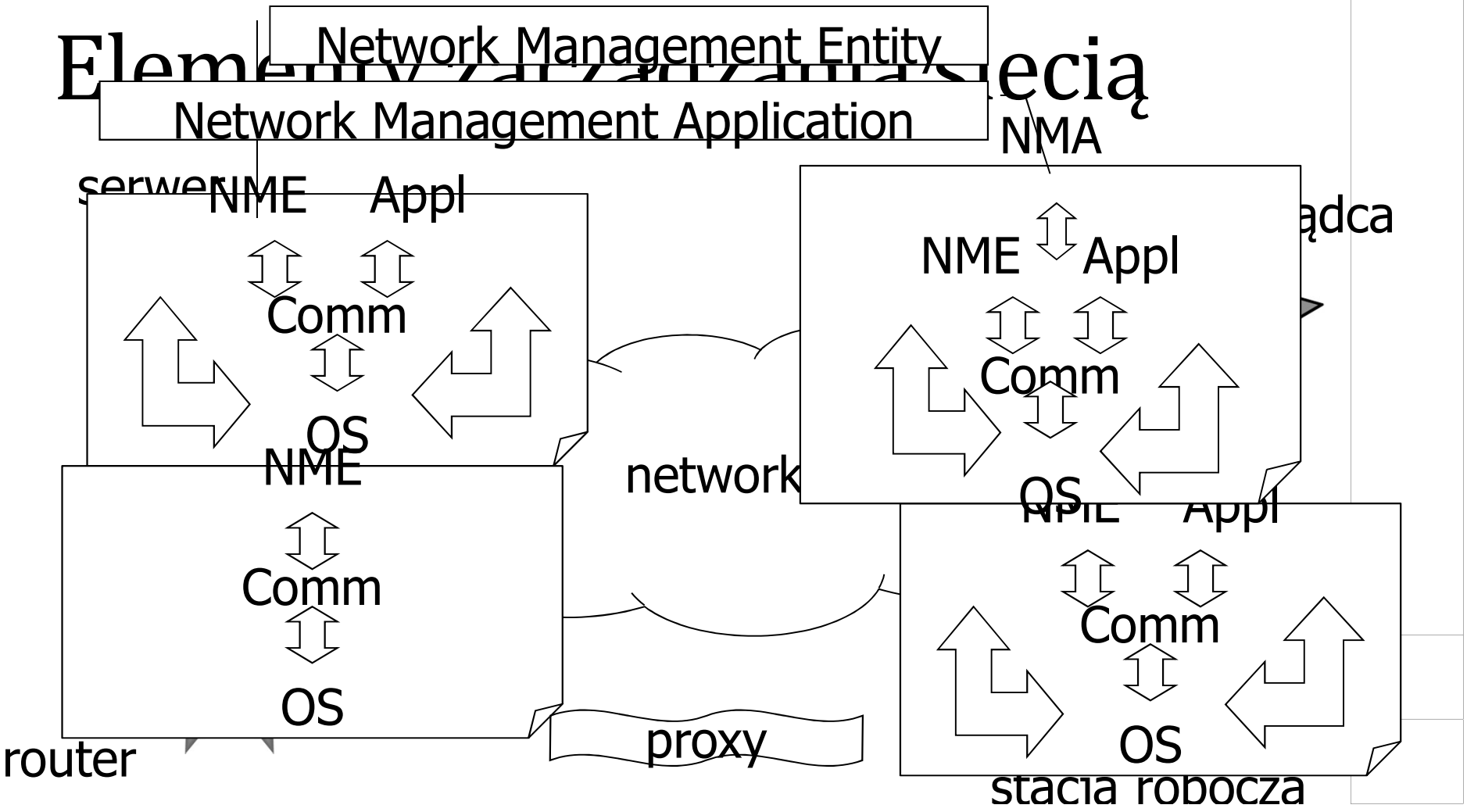
Simple Network Menagement Protocol

- Network monitoring
- Network menagement

SNMP - commands

- Get
- Set
- Trap

Elementy zarządzania siecią

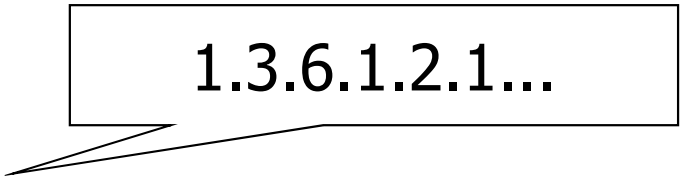


MIB-II assumptions

- important obiect only
- week control object only (to safety)
- no redundancy
- avoiding heavy load on critical sections of code (1 counter in section)

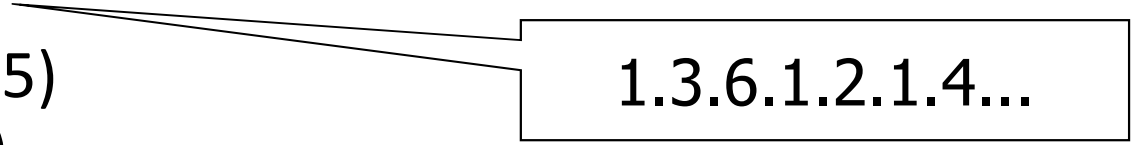
MIB main structure

- iso (1)
  - org (3)
    - dod (6)
      - internet (1)
        - directory (1)
        - mgmt (2)
        - mib-2 (1)
        - experimental (3)
        - private (4)



Structure of MIB-II

- system (1)
- interfaces (2)
- *at (3) – translacja adresów*
- ip (4)
- icmp (5)
- tcp (6)
- udp (7)
- egp (8)
- dot3 (10) – mechanizmy transmisji
- snmp (11)



System (1)

- sysDescr (RO) DisplayString(SIZE(0..255))
- sysObjectID (RO) OBJECT ID
- sysUpTime (RO) TimeTicks
- sysContact (RW) DisplayStri
- sysName (RW) DisplayStrin
- sysLocation (RW) DisplayStr
- sysServices (RO) INTEGER (0..127)

1 – physical (repeater)
2 – data link (bridge)
3 – network (IP router)
4 – host to host (IP hosts)
7 – application (mail exchangers)

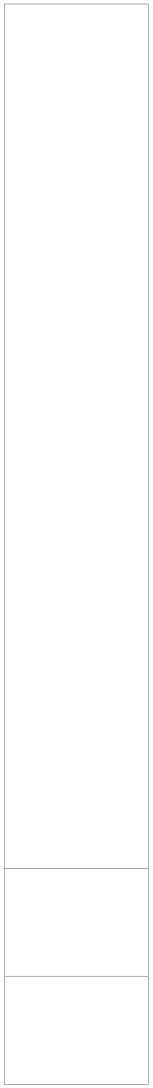
$$\sum_{L \in S} 2^{L-1}$$

Interfaces (2)

- ifNumber
- ifTable
  - ifEntry
    - ifIndex
    - ifDescr
    - ifType
    - ifMtu
    - ifSpeed
    - ifPhysAddress
    - ifAdminStatus (RW)
    - ifOperStatus
    - ifLastChange
    - ifInOctets
    - ifInUcastPkts
    - ifInNUcastPkts
    - ifInDiscards
    - ifInErrors
    - ifInUnknownProtos
    - ifOutOctets
    - ifOutUcastPkts
    - ifOutNUcastPkts
    - ifOutDiscards
    - ifOutErrors
    - ifOutQLen
    - ifSpecific

Ip (4)

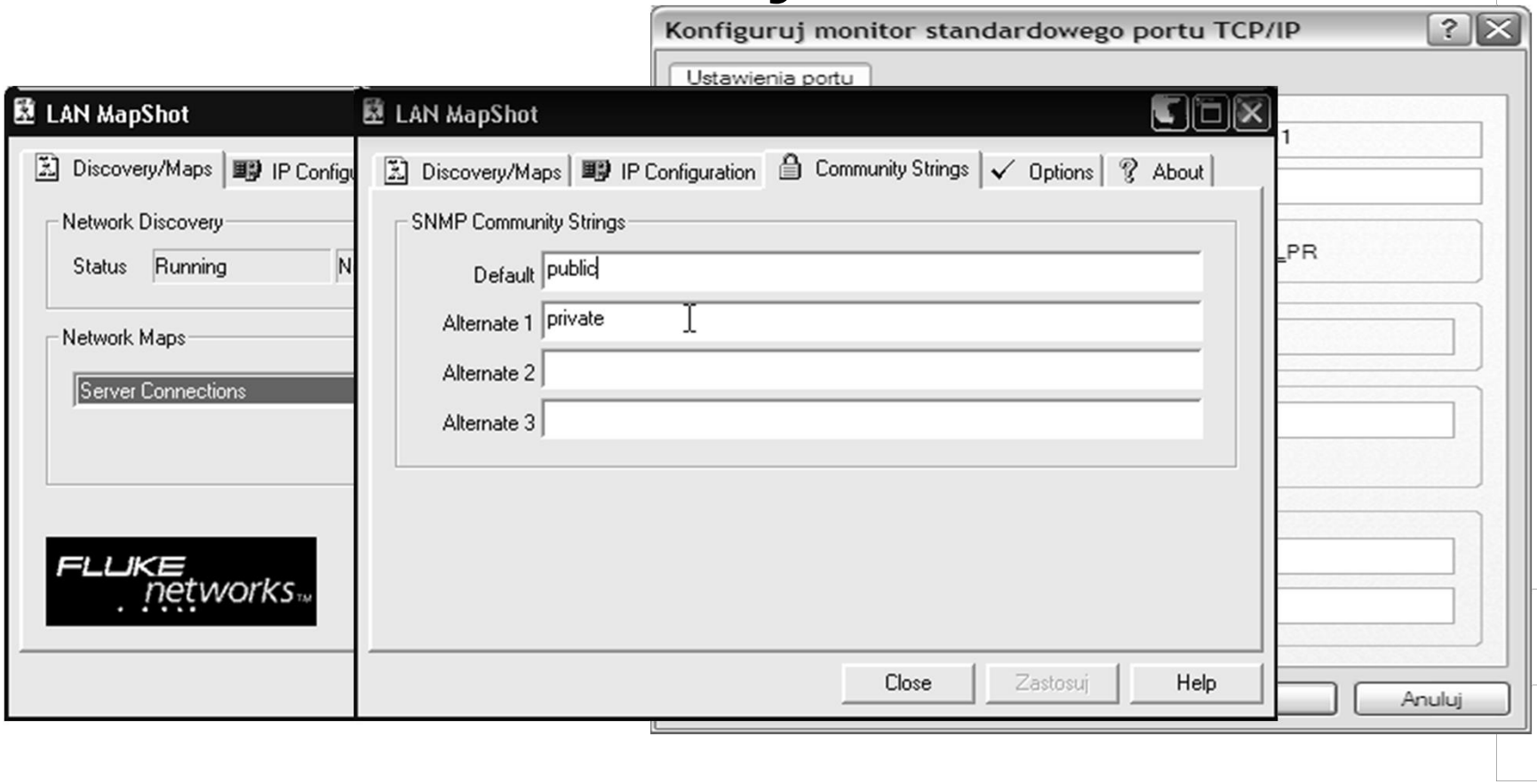
- ipForwarding
- ipDefaultTTL
- ipInReceives
- ipInHdrErrors
- ipInAddrErrors
- ipForwDatagrams
- ipUnknownProtos
- ipInDiscards
- ipInDelivers
- ipOutRequests
- ipOutDiscards
- ipOutNoRoutes
- ipReasmTomeout
- ipReasmReqds
- ipReasmOKs
- ipReasmFails
- ipFragOKs
- ipFragFails
- ipFragCreates



Ip (4) cont

- ipAddrTable
  - ipAddrEntry
    - ipAdEntAddr
    - ipAdEntIfIndex
    - ipAdEntNetMask
    - ipAdEntBcastAddr
    - ipAdEntReasmMaxSize
- ipRouteTable
  - ipRouteEntry
    - ipRouteDest
    - ipRouteIfIndex
    - ipRouteMetric1
    - ipRouteMetric2
    - ipRouteMetric3
    - ipRouteMetric4
    - ipRouteNextHop
    - ipRouteType
    - ipRouteProto
    - ipRouteAge
    - ipRouteMask
    - ipRouteMetric5
    - ipRouteInfo
- ipNetToMediaTable
  - ipNetToMediaEntry
    - ipNetToMediaIfIndex
    - ipNetToMediaPhysAddress
    - ipNetToMediaNetAddress
    - ipNetToMediaType
- ipRoutingDiscards

SNMP community



Access for MIB elements

- view MIB – group of obiects
- access mode SNMP (RO, RW)

MIB	SNMP	
	RO	RW
RO	Get, Trap	
RW	Get, Trap	Get, Set, Trap
WO	*Get, Trap*	*Get*, Set, *Trap*
NA	NA	NA