

Όνοματεπώνυμο: Άγγελος Μητροκώτσας		Ομάδα: 6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2		Ημερομηνία: 8/11/ 2021
Διεύθυνση IP: 192.168.1.8	Διεύθυνση MAC:	F8-63-3F-59-24-C8

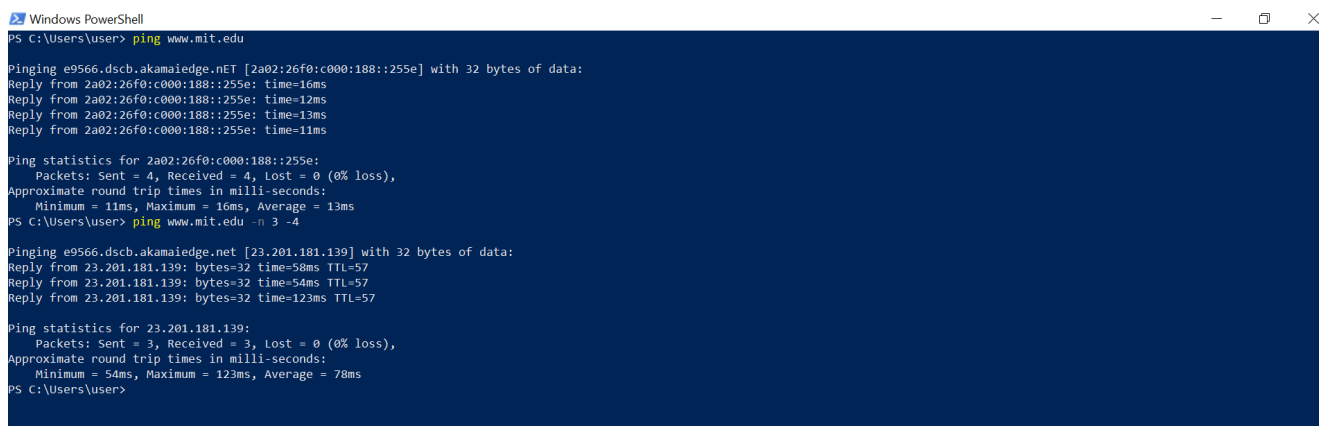
## Εργαστηριακή Άσκηση 4

### Πρωτόκολλο IPv4 και θρυμματισμός

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 ping www.mit.edu -n 3 -4



```
Windows PowerShell
PS C:\Users\user> ping www.mit.edu

Pinging e9566.dscb.akamaiedge.NET [2a02:26f0:c000:188::255e] with 32 bytes of data:
Reply from 2a02:26f0:c000:188::255e: time=16ms
Reply from 2a02:26f0:c000:188::255e: time=12ms
Reply from 2a02:26f0:c000:188::255e: time=13ms
Reply from 2a02:26f0:c000:188::255e: time=11ms

Ping statistics for 2a02:26f0:c000:188::255e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 16ms, Average = 13ms
PS C:\Users\user> ping www.mit.edu -n 3 -4

Pinging e9566.dscb.akamaiedge.net [23.201.181.139] with 32 bytes of data:
Reply from 23.201.181.139: bytes=32 time=58ms TTL=57
Reply from 23.201.181.139: bytes=32 time=54ms TTL=57
Reply from 23.201.181.139: bytes=32 time=123ms TTL=57

Ping statistics for 23.201.181.139:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 123ms, Average = 78ms
PS C:\Users\user>
```

1.2 Δεν θα καταγραφούν τα πλαίσια που απευθύνονται σε πολλούς υπολογιστές του δικτύου στο οποίο βρίσκομαι, με βοηθάει να βλέπω πλαίσια που προέρχονται από ή κατευθύνονται προς το δικό μου υπολογιστή

1.3 Ποσοστό απωλειών Lost = 0 (0% loss) και Average = 78ms η καθυστέρηση

1.4 Reply from 23.201.181.139: bytes=32 time=58ms TTL=57

Reply from 23.201.181.139: bytes=32 time=54ms TTL=57

Reply from 23.201.181.139: bytes=32 time=123ms TTL=57

Approximate round trip times in milli-seconds:

Minimum = 54ms, Maximum = 123ms, Average = 78ms

The screenshot shows the Wireshark interface with a packet capture of ICMP ping requests and replies. The packet list shows frames 20 through 27. Frame 20 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the selected frame.

No.	Time	Source	Protocol	Length	Destination	Info
20	0.018635	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (
21	0.058599	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=37/9472, ttl=57 (r
22	0.963276	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (
23	0.054693	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=38/9728, ttl=57 (r
24	0.972202	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (
25	0.122688	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=39/9984, ttl=57 (r
26	0.323163	192.168.1.8	TCP	66	20.54.232.160	53478 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
27	0.070099	20.54.232.160	TCP	66	192.168.1.8	443 → 53478 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{11981F20-5231-4861-ABD2-DD8A4A767CB9}

Ethernet II, Src: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)

Internet Protocol Version 4, Src: 192.168.1.8, Dst: 23.201.181.139

Internet Control Message Protocol

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$...E.  
0010 00 3c 61 52 00 00 80 01 4a 6a c0 a8 01 08 17 c9 <aR... Jj.....  
0020 b5 8b 08 00 4d 36 00 01 00 25 61 62 63 64 65 66 ....M6... %abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

wireshark\_Wi-Fi3G5LC1.pcapng | Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Οι τιμές των Round Trip Time από το παράθυρο εντολών και από το Wireshark συμφωνούν μεταξύ τους.

## 1.6 Το ip

## 1.7 Το icmp

## 1.8 Στάλθηκαν requests

## 1.9 Πηγή : 192.168.1.8, Προορισμός: 23.201.181.139

The screenshot shows the Wireshark interface with a packet capture of ICMP ping requests and replies. The packet list shows frames 20 through 25. Frame 20 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the selected frame.

No.	Time	Source	Protocol	Length	Destination	Info
20	0.000000	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply
21	0.058599	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=37/9472, ttl=57 (request
22	0.963276	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply
23	0.054693	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=38/9728, ttl=57 (request
24	0.972202	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply
25	0.122688	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=39/9984, ttl=57 (request

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{11981F20-5231-4861-ABD2-DD8A4A767CB9}

Ethernet II, Src: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)

Destination: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)

Source: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8)

Type: IPv4 (0x0800)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$...E.  
0010 00 3c 61 52 00 00 80 01 4a 6a c0 a8 01 08 17 c9 <aR... Jj.....  
0020 b5 8b 08 00 4d 36 00 01 00 25 61 62 63 64 65 66 ....M6... %abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Internet Control Message Protocol: Protocol | Packets: 51 · Displayed: 6 (11.8%) · Dropped: 0 (0.0%) | Profile: Default

## 1.10 Ελήφθη σαν replies

## 1.11 Πηγή :23.201.181.139, Προορισμός: 192.168.1.8

1.12 Έχει αλλάξει η διεύθυνση της πηγής (του αποστολέα) των requests και προορισμού των replies. Αλλάζει και ο RTT των πακέτων.

Wireshark packet capture showing ICMP ping requests and replies. The packet list shows a sequence of requests and replies with changing source and destination IP addresses. The packet details pane shows the structure of an ICMP Echo (ping) request and reply. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Protocol	Length	Destination	Info
14	1.011565	2a02:587:2129:d827::...	ICMPv6	94	2a02:26f0:c000:188::...	Echo (ping) request id=0x0001, seq=272, hop limit=128
15	0.011576	2a02:26f0:c000:188::...	ICMPv6	94	2a02:587:2129:d827::...	Echo (ping) reply id=0x0001, seq=272, hop limit=59 (re
16	3.373597	2a02:587:2129:d827::...	TCP	75	2a02:26f0:c000:1a4::...	53472 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segme
17	0.029412	2a02:26f0:c000:1a4::...	TCP	86	2a02:587:2129:d827::...	443 → 53472 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=
18	0.143599	fe80::451b:e6fd:ee4::...	DNS	91	fe80::1	Standard query 0xc5db A www.mit.edu
19	0.028970	fe80::1	DNS	191	fe80::451b:e6fd:ee4::...	Standard query response 0xc5db A WwW.mIT.Edu CNAME ww
20	0.018635	192.168.1.8	ICMP	74	23.201.181.139	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (
21	0.058599	23.201.181.139	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=37/9472, ttl=57 (r

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{11981F20-5231-4861-ABD2-DD8A4A767CB} Ethernet II, Src: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)

Destination: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)

Source: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8)

Type: IPv4 (0x0800)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$...E.  
 0010 00 3c 61 52 00 00 80 01 4a 6a c0 a8 01 08 17 c9 .<aR.... Jj.....  
 0020 b5 8b 08 00 4d 36 00 01 00 25 61 62 63 64 65 66 ....M6...%abcdef  
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
 0040 77 61 62 63 64 65 66 67 68 69 wabcdfg hi

Frame (frame), 74 byte(s) | Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

## 2

2.1 i. ping 192.168.1.1 -n 5 -4

ii. ping 192.168.1.8 -n 5 -4

iii. ping 127.0.0.1 -n 5 -4

```

PS C:\Users\user> ping 192.168.1.1 -n 5 -4

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 5ms
PS C:\Users\user> ping 192.168.1.8 -n 5 -4

Pinging 192.168.1.8 with 32 bytes of data:
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\user> ping 127.0.0.1 -n 5 -4

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\user>
  
```

OneDrive  
Το στιγμιότυπο οθόνης αποθηκεύτηκε  
Το στιγμιότυπο οθόνης προστέθηκε στο OneDrive.

2.2 Το wireshark έχει καταγράψει μόνο 5 requests από τα 15 που έστειλε ο υπολογιστής μας

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Protocol	Length	Destination	Info
83	0.000000	192.168.1.8	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=97/24832, ttl=128 (reply
84	0.002885	192.168.1.1	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=97/24832, ttl=64 (request
96	1.006699	192.168.1.8	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (reply
97	0.006694	192.168.1.1	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=98/25088, ttl=64 (request
111	1.020817	192.168.1.8	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=99/25344, ttl=128 (reply
112	0.005588	192.168.1.1	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=99/25344, ttl=64 (request
120	1.020962	192.168.1.8	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=100/25600, ttl=128 (reply
121	0.004918	192.168.1.1	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=100/25600, ttl=64 (request
132	1.018169	192.168.1.8	ICMP	74	192.168.1.1	Echo (ping) request id=0x0001, seq=101/25856, ttl=128 (reply
133	0.005333	192.168.1.1	ICMP	74	192.168.1.8	Echo (ping) reply id=0x0001, seq=101/25856, ttl=64 (request

> Frame 83: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{11981F20-5231-4861-ABD2-DD8A4A767CB} <

> Ethernet II Src: IntelCor 59:24:c8:f8:63:3f Dst: Sercomm f7:d3:40:38:02:de <

```

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y$...E.
0010 00 3c af 59 00 00 80 01 08 0e c0 a8 01 08 c0 a8 <..Y.....
0020 01 01 08 00 4c fa 00 01 00 61 61 62 63 64 65 66 ....L... aabcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefg hi

```

4.2.pcapng | Packets: 340 · Displayed: 10 (2.9%) | Profile: Default

### 2.3 Η προκαθορισμένη πύλη (default gateway)

2.4 Δεν παρατήρησα (δεν καταγράφηκαν) μηνύματα ICMP echo requests με πηγή την IPv4 διεύθυνση του υπολογιστή μου επειδή αυτά τα πακέτα δεν βγήκαν ποτέ στο τοπικό μου δίκτυο όταν εκτέλεσα την εντολή ping προς τον υπολογιστή μου. Ο οδηγός Ethernet αναγνώρισε τη διεύθυνση IPv4 του υπολογιστή μου και την έστειλε στον οδηγό loopback.

2.5 Δεν παρατήρησα (δεν καταγράφηκαν) τέτοια μηνύματα, καθώς όταν εκτέλεσα την εντολή ping προς τη διεύθυνση loopback (του βρόγχου επιστροφής) τα μηνύματα αυτά στάλθηκαν στον οδηγό loopback.

2.6 Όταν κάνω ping προς τη διεύθυνση loopback, τα πακέτα δεν θα μουν ποτέ στον οδηγό Ethernet και βασικά δεν θα φύγουν από τον υπολογιστή μου, καθώς θα μουν στον οδηγό loopback και θα επιστρέψουν στο μηχανήμα μου. Όταν εκτελώ την εντολή ping προς τη διεπαφή του υπολογιστή μου, τα πακέτα μπαίνουν πρώτα στον οδηγό ethernet και επιστρέφουν στον οδηγό loopback (δεν πάνε απευθείας εκεί όπως στην προηγούμενη περίπτωση).

2.7 Ενώ στον φυλλομετρητή ανοίγει κανονικά η σελίδα netflix.com, όταν εκτελώ την εντολή ping προς τον εξυπηρετητή [www.netflix.com](http://www.netflix.com) βλέπω ότι δεν απαντάει στα ping requests (δε λαμβάνω reply, έχω 100% loss). Υποθέτω πως για προστασία από επιθέσεις που δύναται να προέρχονται από το υποδίκτυο του προορισμού γίνεται μπλοκάρισμα όλων των πακέτων με πρωτόκολλο ICMP .

### 3

3.1 host 147.102.40.15

3.2 ip.src==192.168.1.8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.8

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.8	TCP	66	147.102.40.15	55024 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
3	0.013752	192.168.1.8	TCP	54	147.102.40.15	55024 → 23 [ACK] Seq=1 Ack=1 Win=131072 Len=0
5	0.035964	192.168.1.8	TELNET	57	147.102.40.15	Telnet Data ...
7	0.014163	192.168.1.8	TELNET	62	147.102.40.15	Telnet Data ...
9	0.014049	192.168.1.8	TELNET	57	147.102.40.15	Telnet Data ...
11	0.112712	192.168.1.8	TELNET	72	147.102.40.15	Telnet Data ...
13	0.014755	192.168.1.8	TELNET	63	147.102.40.15	Telnet Data ...
15	0.127204	192.168.1.8	TELNET	70	147.102.40.15	Telnet Data ...

> Frame 11: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{11981F20-5231-4861-ABD2-DD8A4A767CB} ^  
 > Ethernet II, Src: IntelCor\_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm\_f7:d3:40 (38:02:de:f7:d3:40)  
 > Internet Protocol Version 4, Src: 192.168.1.8, Dst: 147.102.40.15  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)

0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8...@.c ?Y\$...E.  
 0010 00 3a 98 f5 40 00 80 06 e4 a2 c0 a8 01 08 93 66 :...@... ..f  
 0020 28 0f d6 f0 00 17 7b 25 85 13 c3 78 cc 54 50 18 (. ...{ % ..x TP  
 0030 02 00 74 2b 00 00 ff fb 18 ff fb 1f ff fc 20 ff ..t+... ..  
 0040 fc 23 ff fb 27 ff fc 24 .#...'..\$

Internet Protocol Version 4 (ip), 20 byte(s) | Packets: 123 · Displayed: 67 (54.5%) · Dropped: 0 (0.0%) | Profile: Default

3.3 Version 4 bits

Header length 4 bits

Differentiated Services Field 1 byte

Total length 2 bytes

Identification 2 bytes

Flags 3 bits

Fragment Offset 13 bits

Time to Live 1 byte

Protocol 1 byte

Header Checksum 2 bytes

Source Address 4 bytes

Destination Address 4 bytes

3.4 Τα πεδία DS Field, total length, Identification, Time to Live, Header Checksum, Source Address και Destination Address

3.5 Ναι, Header Length = 20 bytes

3.6 54 bytes το μικρότερο, 80 bytes το μεγαλύτερο

3.7

3.8 Διαφέρουν για το κάθε πακέτο

3.9 Πάντα 1

3.10 Πάντα 0

3.11 Έχει τιμή 6, που αντιστοιχεί στο πρωτόκολλο TCP

3.12 Το checksum εξαρτάται από το άθροισμα των πεδίων της επικεφαλίδας IPv4, επομένως αφού πολλά πεδία της επικεφαλίδας παίρνουν διαφορετικές τιμές από πακέτο σε πακέτο, θα αλλάζει και το checksum.

**4**

4.1	.....
4.2	.....
4.3	.....
4.4	.....
4.5	.....
4.6	.....
4.7	.....
	.....
4.8	.....
4.9	.....
4.10	.....
4.11	.....
4.12	.....
	.....
4.13	.....
	.....
	.....
	.....
	.....
4.14	.....
4.15	.....
4.16	.....
4.17	.....
4.18	.....
4.19	.....
4.20	.....
	.....
4.21	.....
	.....
4.22	.....
	.....
	.....