

# Протокол IP

# Сетевой уровень в стеке TCP/IP

7	Уровень приложения
6	Уровень представления
5	Уровень соединения
4	Транспортный уровень
3	Сетевой уровень
2	Канальный уровень
1	Физический уровень

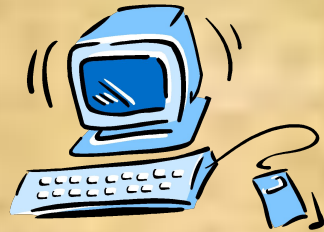
TELNET, FTP, DNS, другие
TCP, UDP
IP, ICMP

# Идентификация узлов

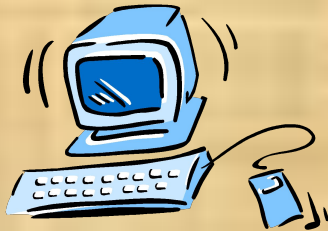
IP-адрес



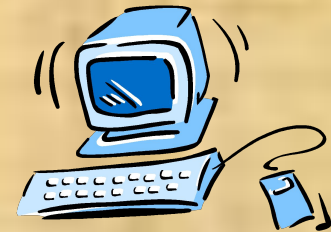
IP-адрес



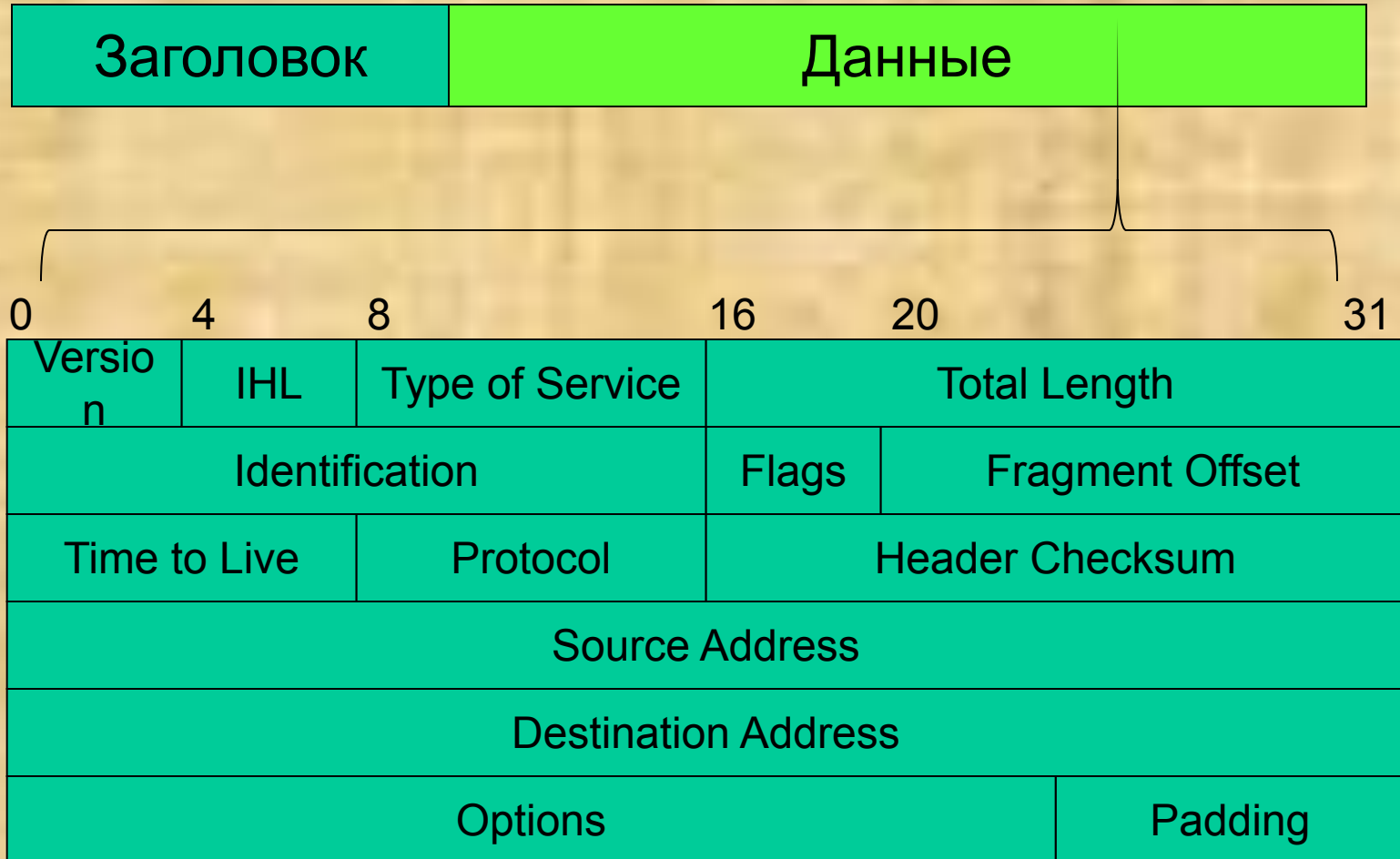
IP-адрес



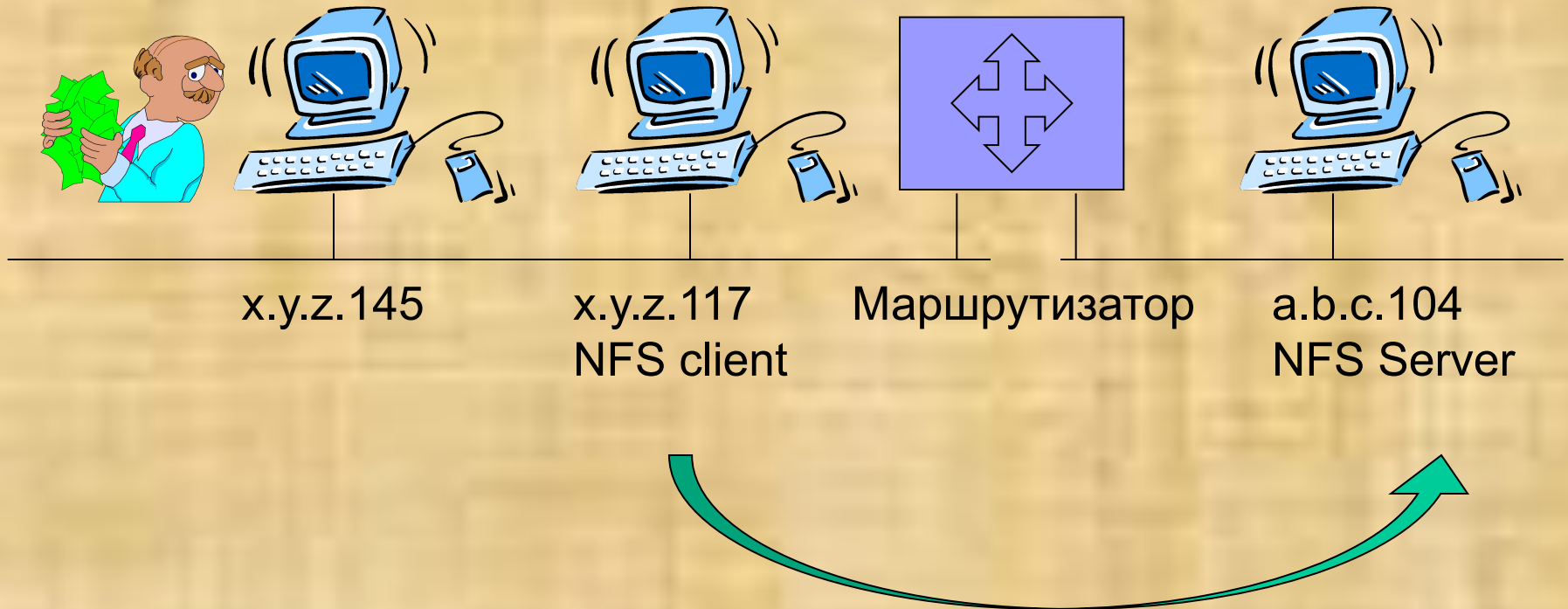
IP-адрес



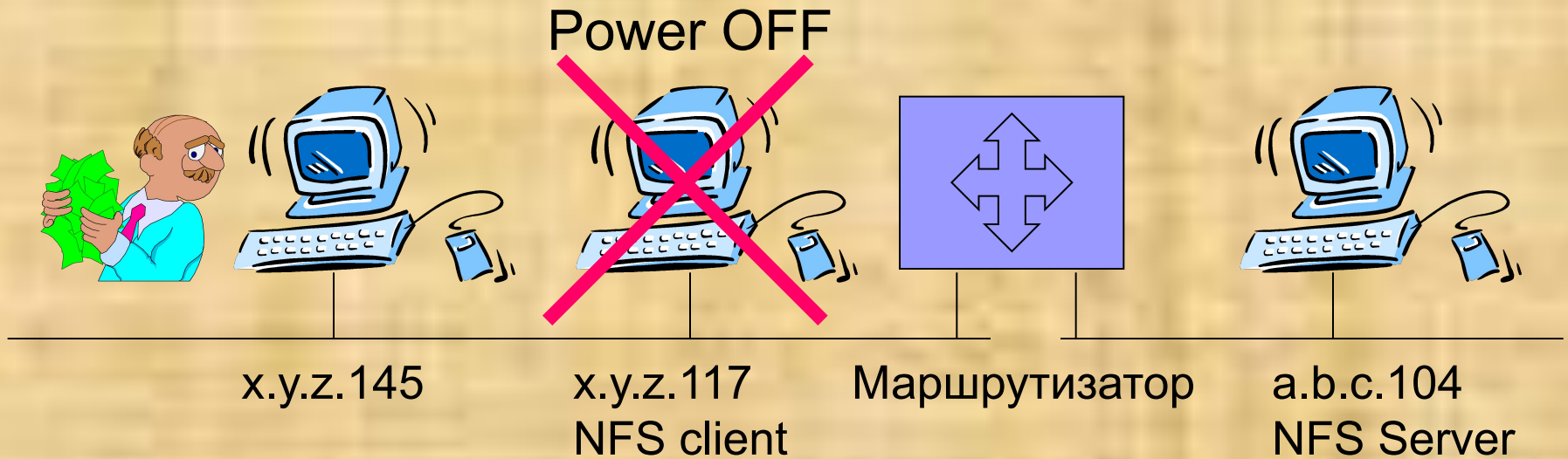
# Формат заголовка IP-пакета



# Атака Address Masquerading

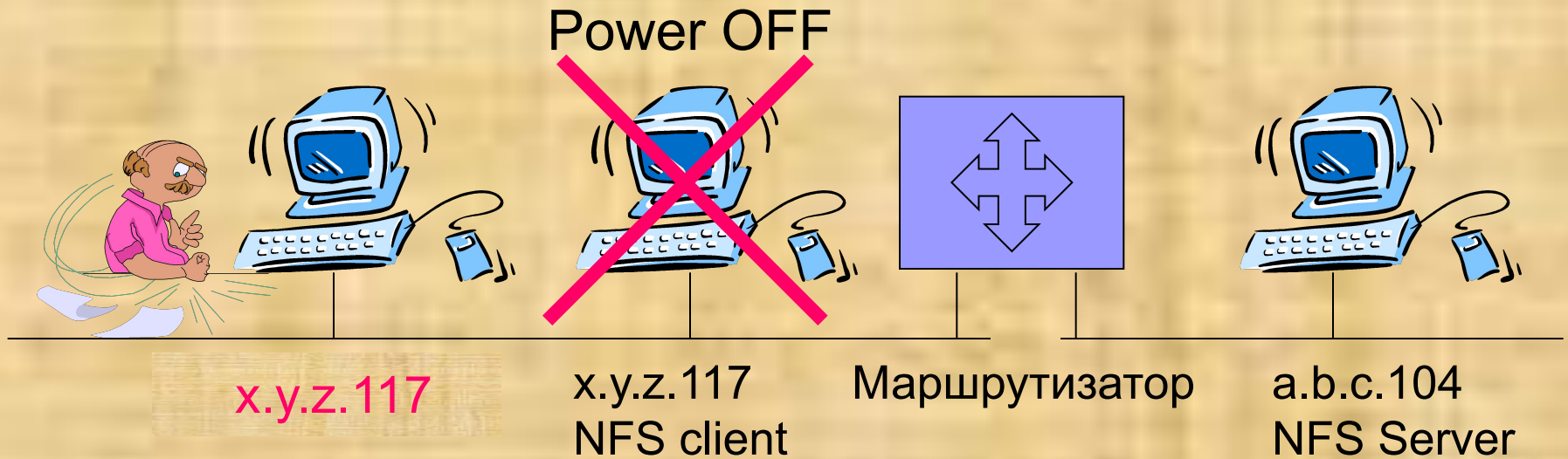


# Атака Address Masquerading

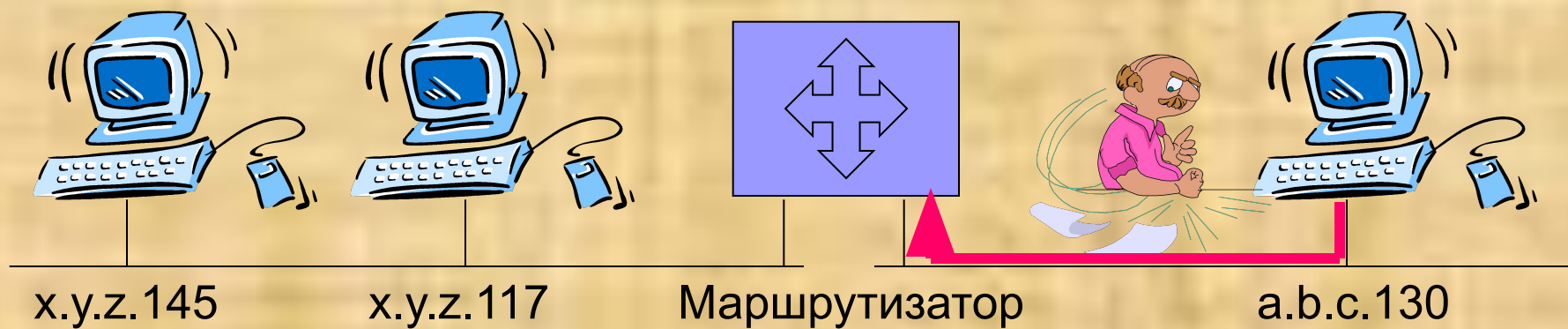




# Атака Address Masquerading

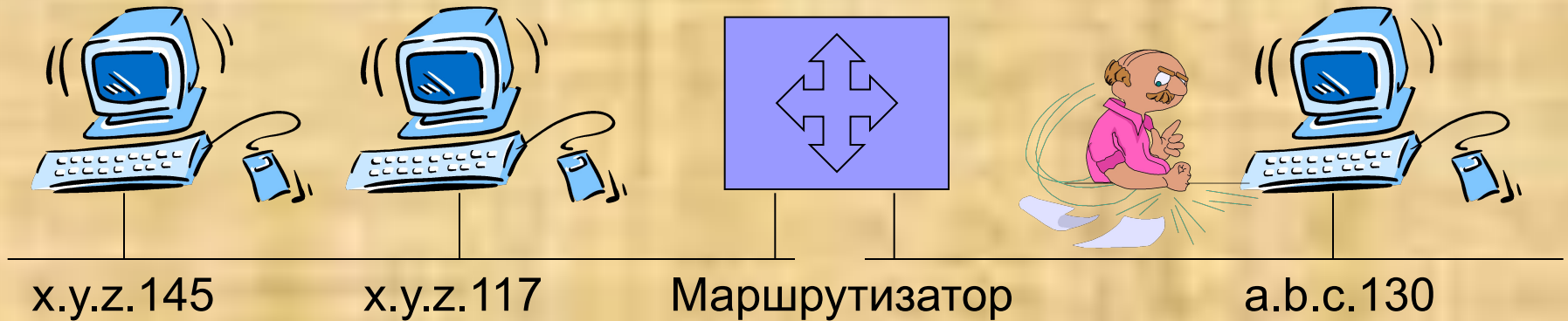


# Address Spoofing



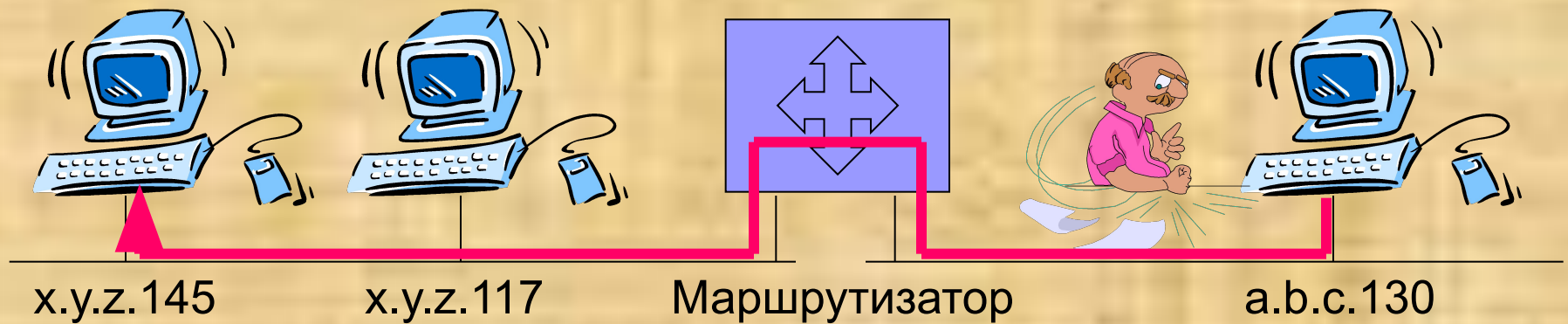


# Address Spoofing

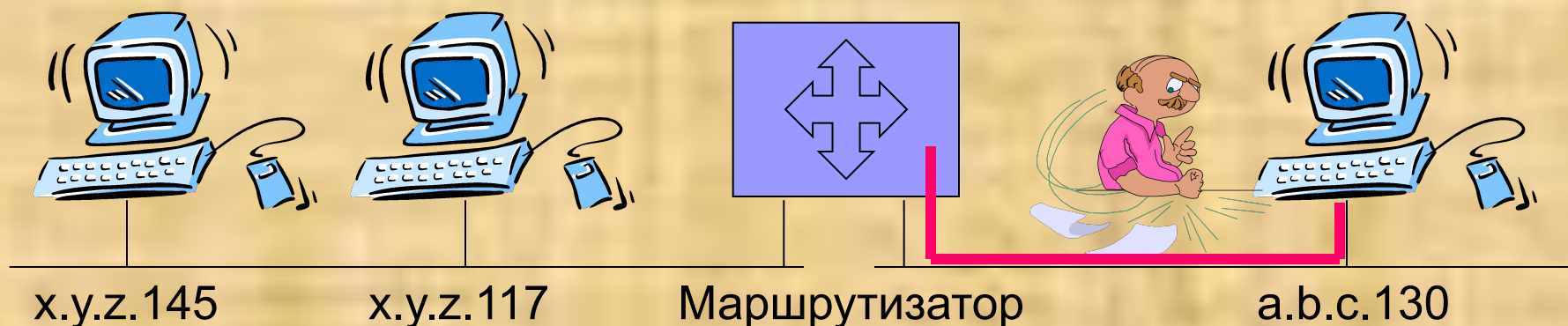


Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
x.y.z.120				
x.y.z.145				
Options				Padding

# Address Spoofing (IPSpoofing)

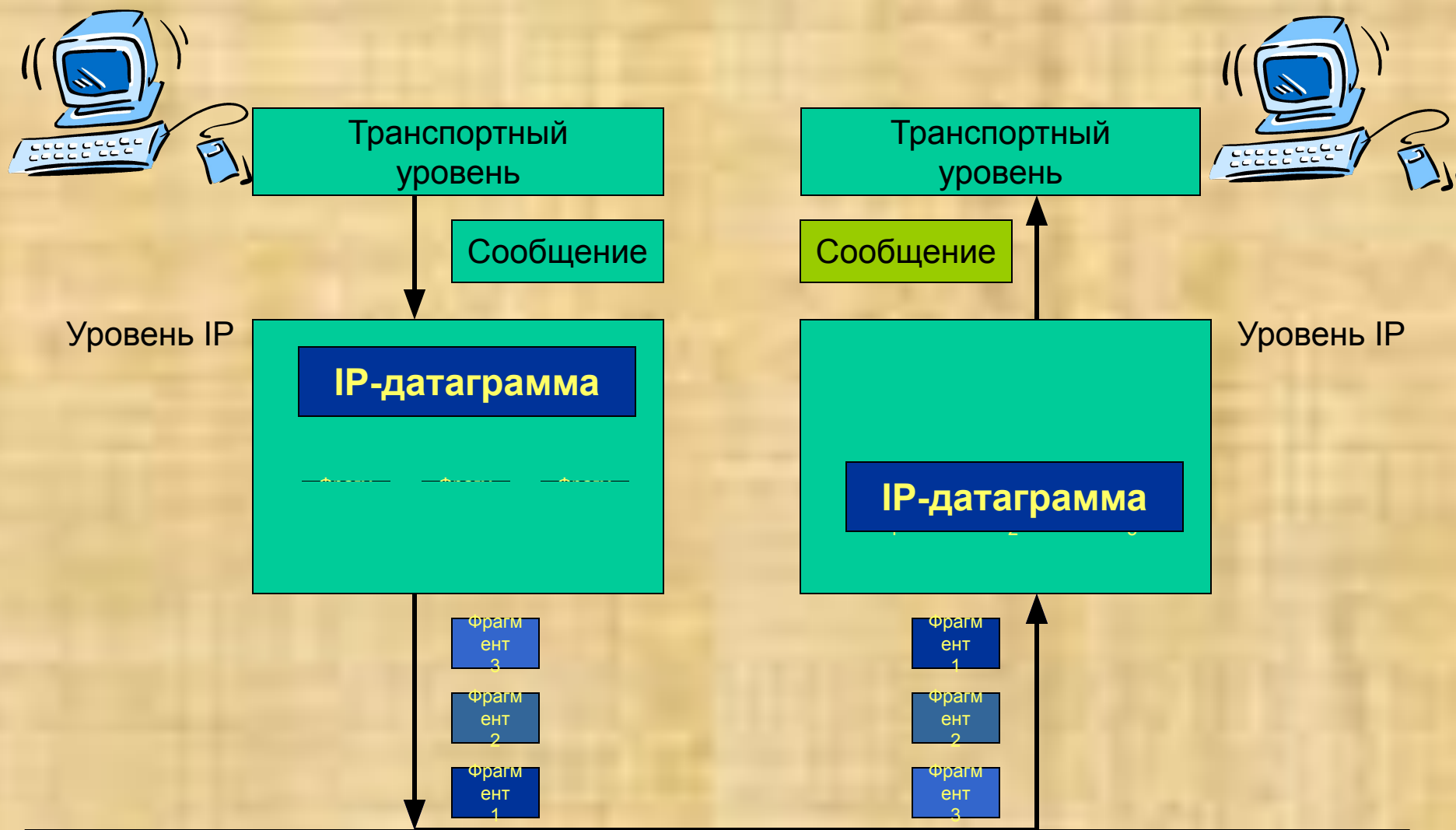


# Адреса источника, подлежащие фильтрации

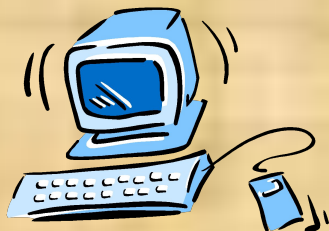


1. Адрес данного узла
2. Адреса, рекомендуемые для внутренних сетей
3. Адреса для группового вещания (224.0.0.0 – 239.255.255.255)
4. Адреса класса Е (240.0.0.0 – 247.255.255.255)
5. Адреса типа «обратная петля» 127.x.x.x
6. Некорректные адреса (например, 0.0.0.0)

# Фрагментация



# Фрагментация



~~C:\>ping 200.200.200.200 -l 4000~~

20

8

4000

**Заголовок  
IP**

**Заголовок  
ICMP  
(эхо-запрос)**

**Данные  
ICMP**

4028

# Фрагментация

20

8

4000



Первый  
фрагмент

20

8

1472



Второй  
фрагмент

20

1500

1480





# Фрагментация

20

8

1472

Первый  
фрагмент

**Заголовок  
IP**

**Заголовок  
ICMP  
(эхо-запрос)**

**Данные  
ICMP**

1500

Второй  
фрагмент

20

1480

**Заголовок  
IP**

**Данные  
ICMP**

20

1048

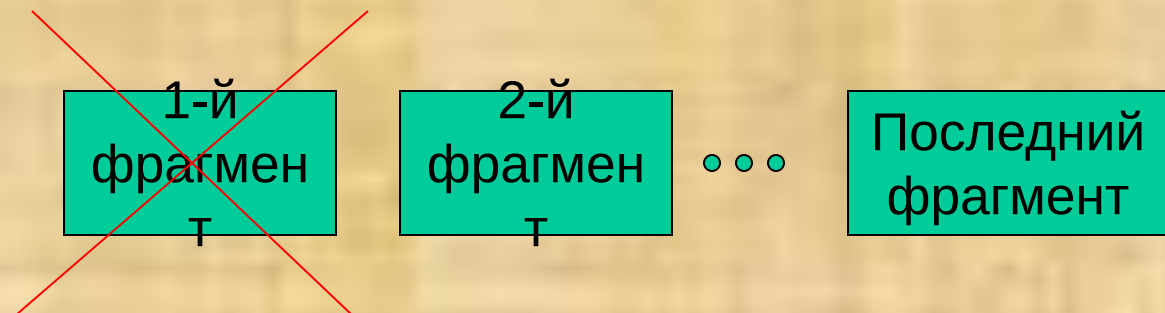
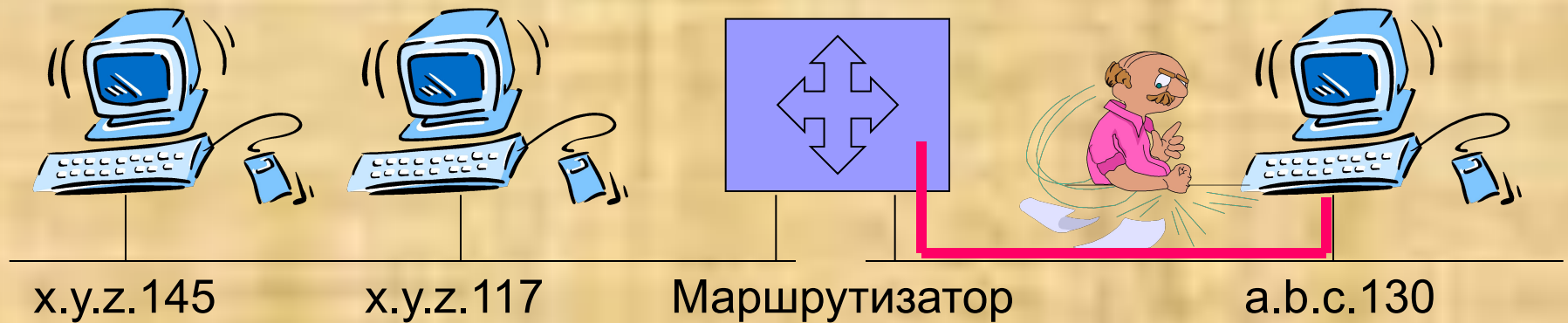
Последний  
фрагмент

**Заголовок  
IP**

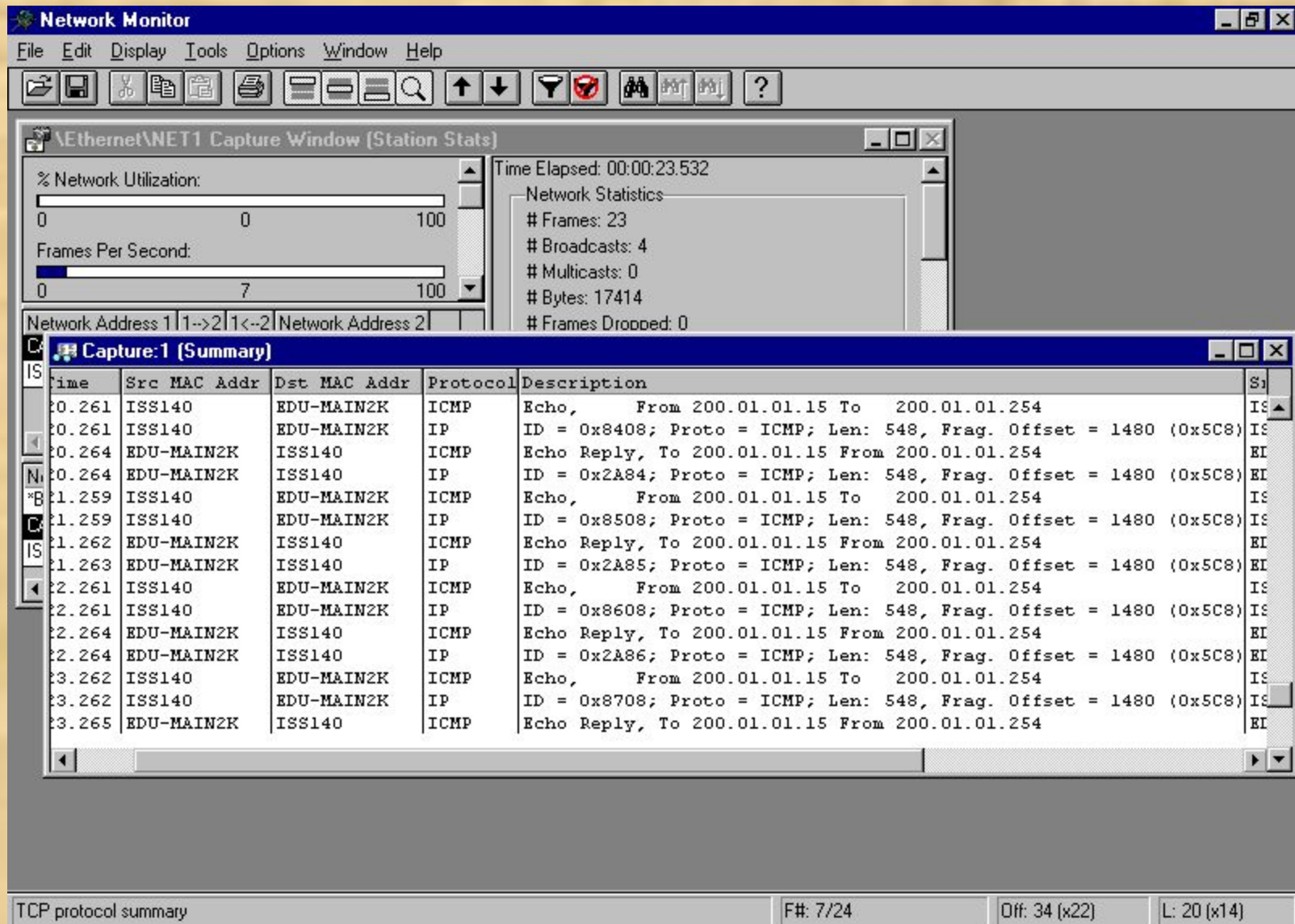
**Данные  
ICMP**

214

# Фрагментация с целью обхода фильтрации



# Фрагментация с целью обхода фильтрации



# **Ошибки реализации функции фрагментации**

**Атака Teardrop**

**Атака IP DoS Fragmenting (jolt2)**

**Атака Ping of Death**

# Фрагментация

Заголовок исходной датаграммы (до фрагментации)

Ver	IHL	ToS	Total Length=472	
Identification=333			Flags =0	Fragment Offset=0

Заголовок=20 байт

Данные=452 байта

Заголовок 1-го фрагмента

Ver	IHL	ToS	Total Length=276	
333			1	0

Flags= 0 0 1    Данные=256 байт

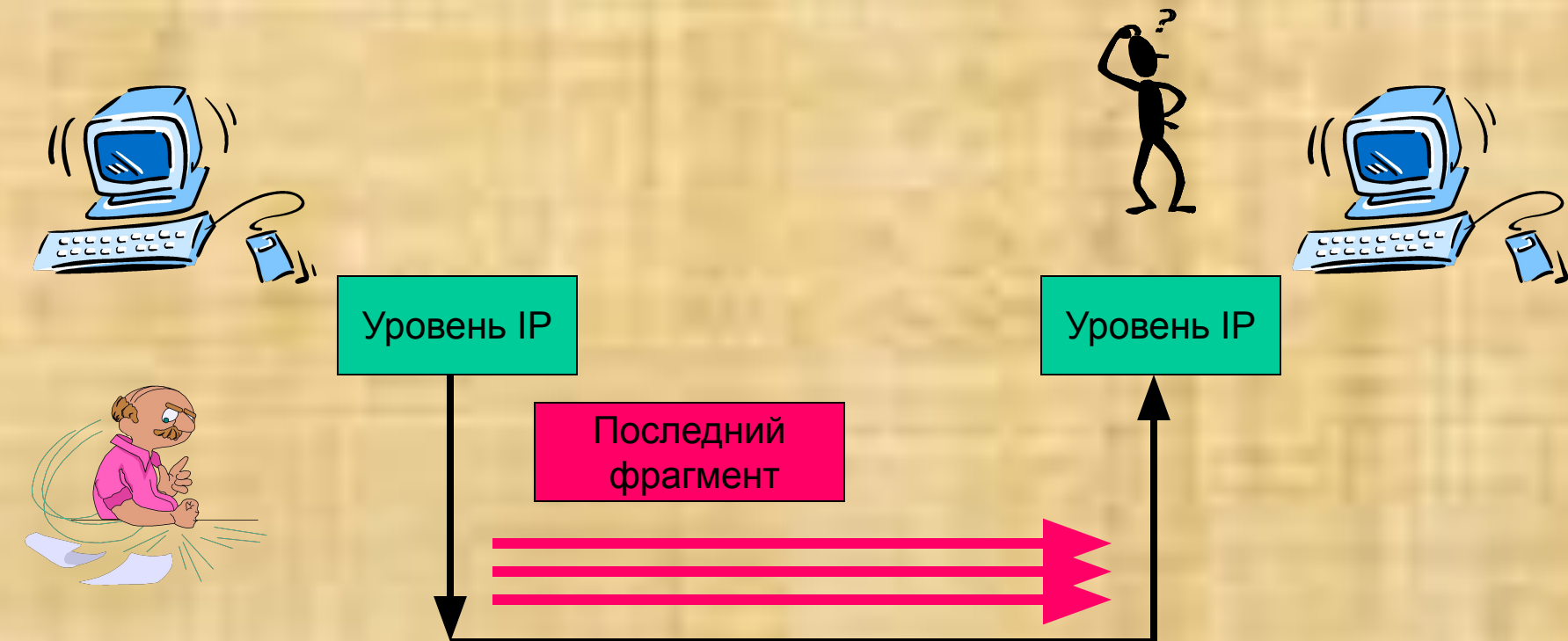
Заголовок 2-го фрагмента

Ver	IHL	ToS	Total Length=216	
333			0	240

Данные=196 байт

есть следующий  
фрагмент

# Ошибки реализации функции фрагментации



**Атака IP DoS Fragmenting (jolt2)**



# Атака Ping of Death

Type=8 или 0	Code=0	Checksum
Идентификатор		Номер
Сообщение (данные пакета)		

```
C:\WINDOWS>ping 200.1.1.1 -l 65535
```

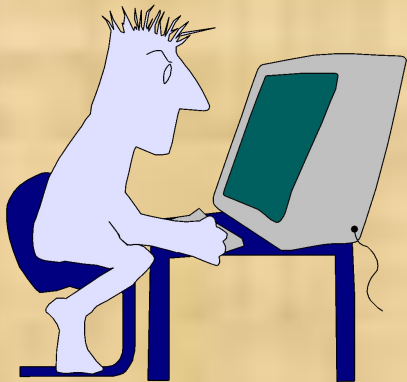
```
Pinging 200.1.1.1 with 32 bytes of data:
```

```
Reply from 200.1.1.1: bytes=32 time<10ms TTL=32
```

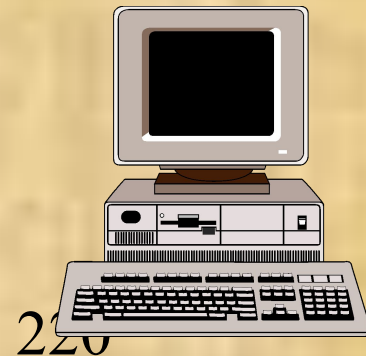
```
Reply from 200.1.1.1: bytes=32 time<10ms TTL=32
```

```
Reply from 200.1.1.1: bytes=32 time<10ms TTL=32
```

```
Reply from 200.1.1.1: bytes=32 time<10ms TTL=32
```



Сообщения «Эхо-запрос»/«Эхо-ответ»



# **Атаки на протокол ICMP**

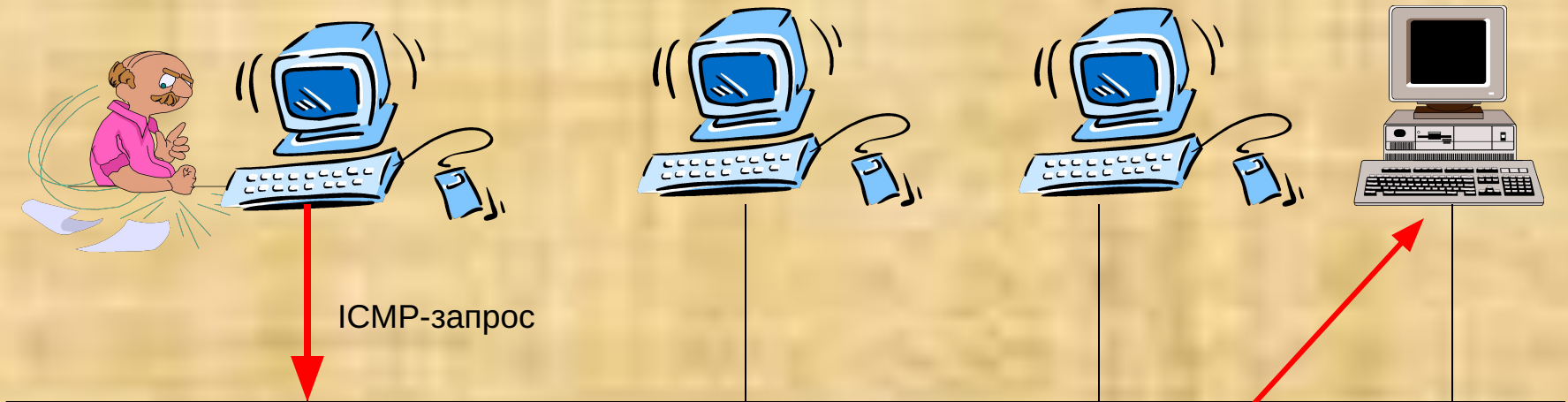
**ICMP Subnet Mask Address Request**

**ICMP Redirect**

**ICMP Timestamp**

**Smurf**

# Атака Smurf

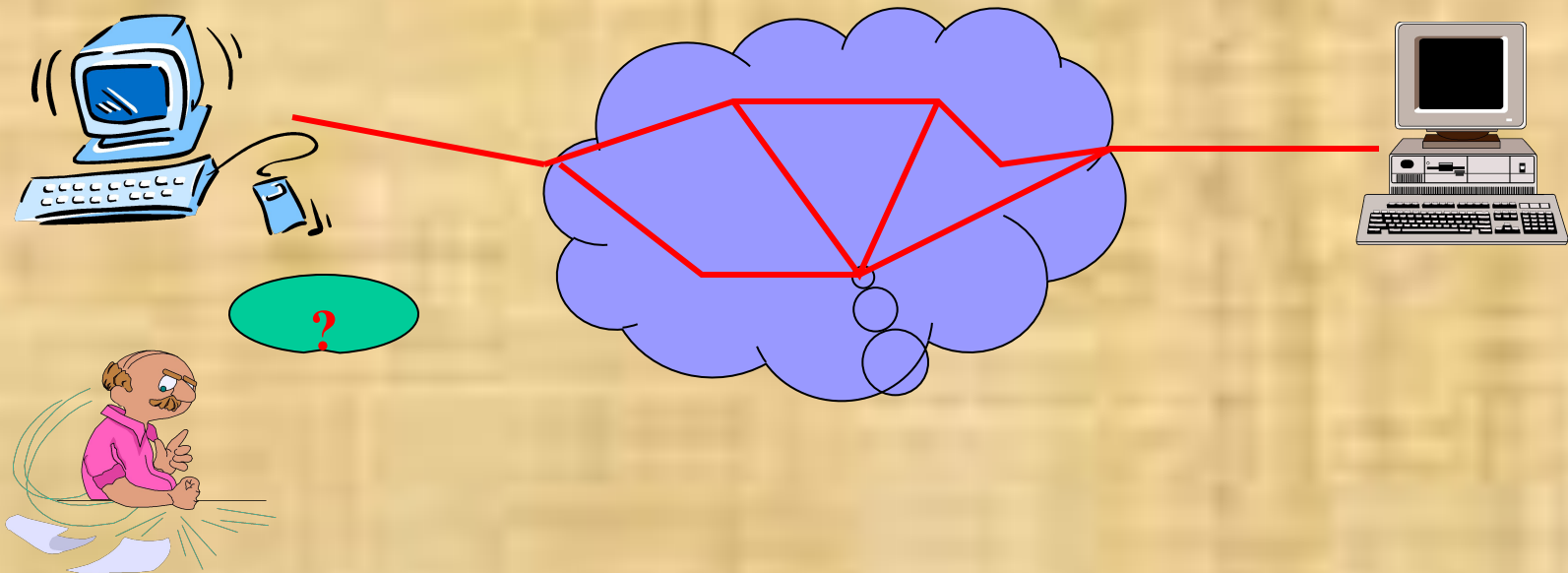


Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol=ICMP		Header Checksum	
Адрес объекта атаки				
Адрес сети или широковещательный				
Options				Padding

# Атака Smurf



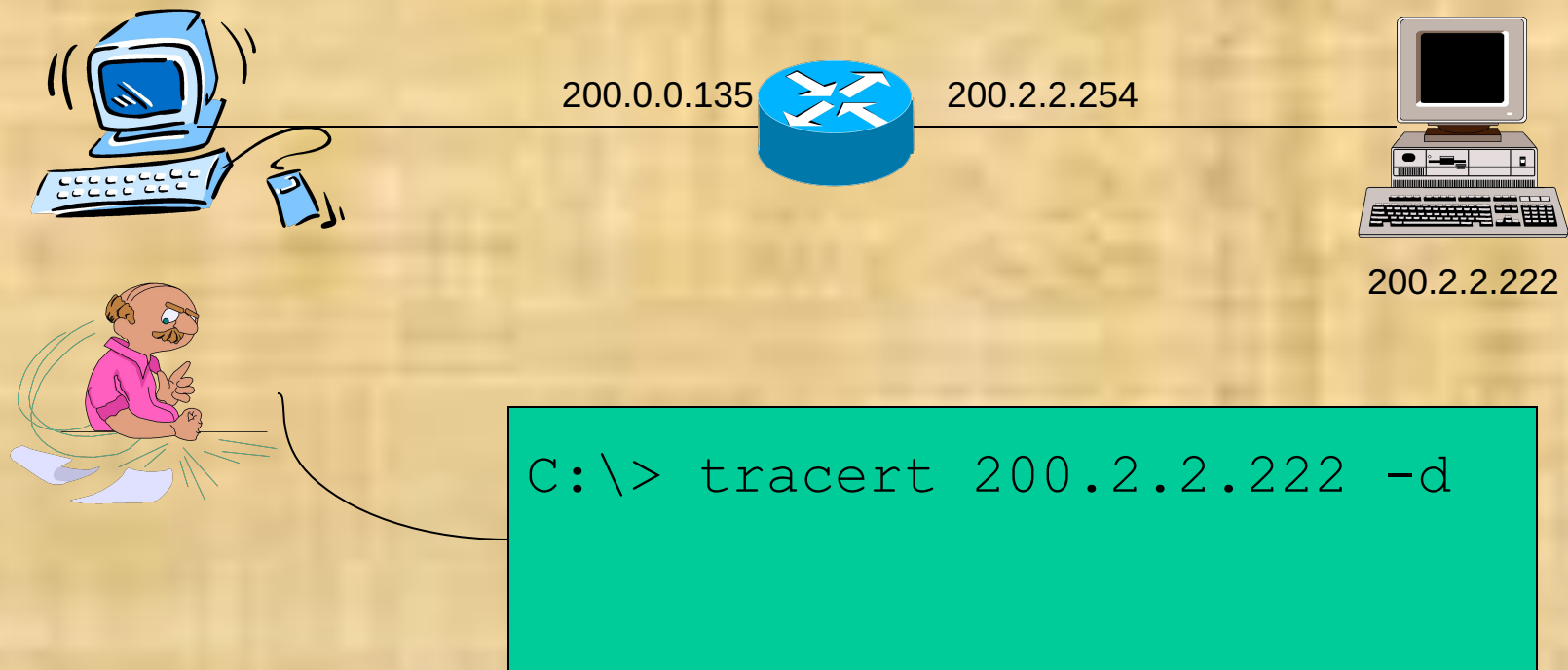
# Отслеживание маршрутов



- Протокол ICMP
- Протокол UDP

# Отслеживание маршрутов - пример

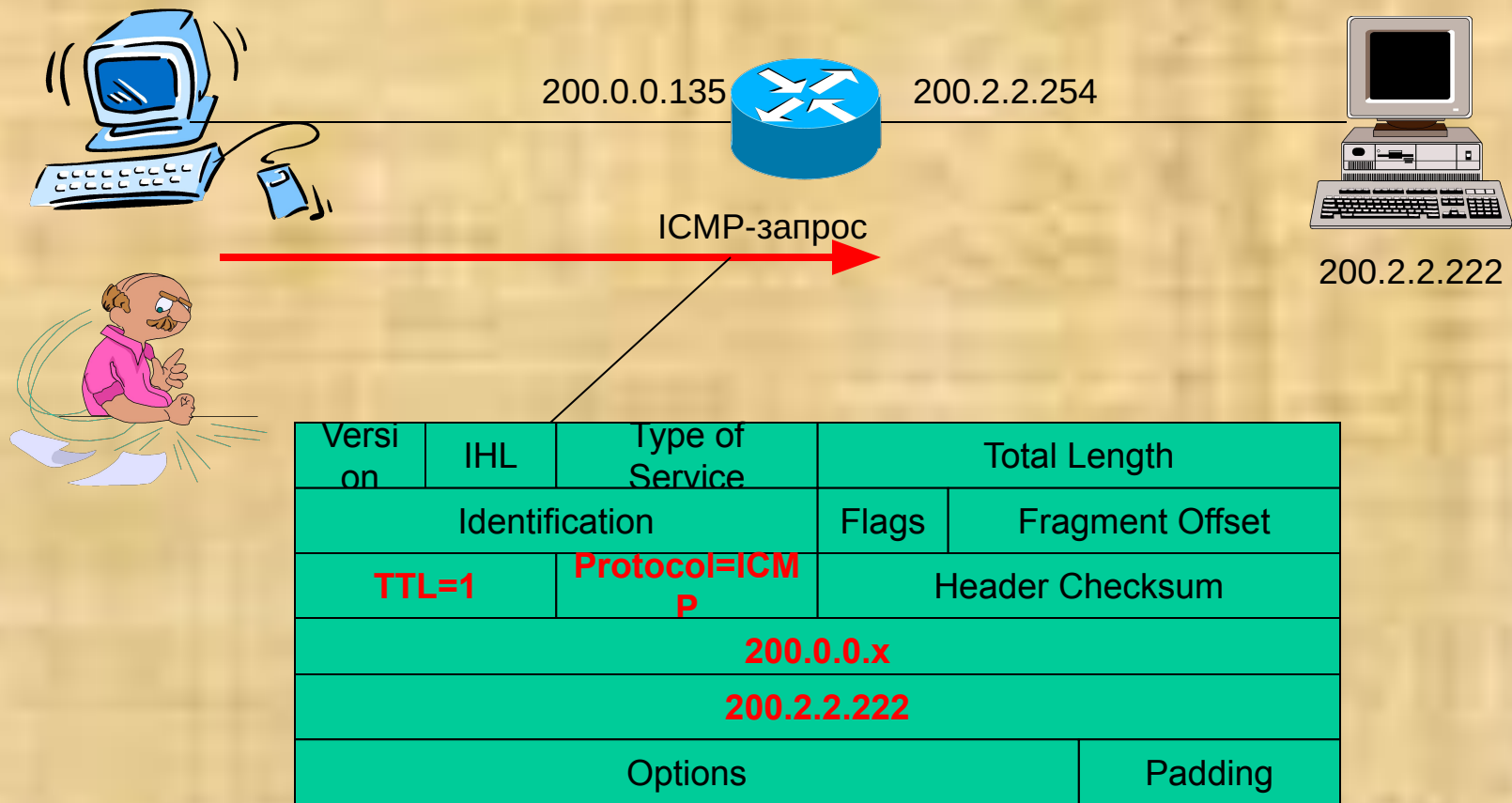
Windows – утилита **tracert**





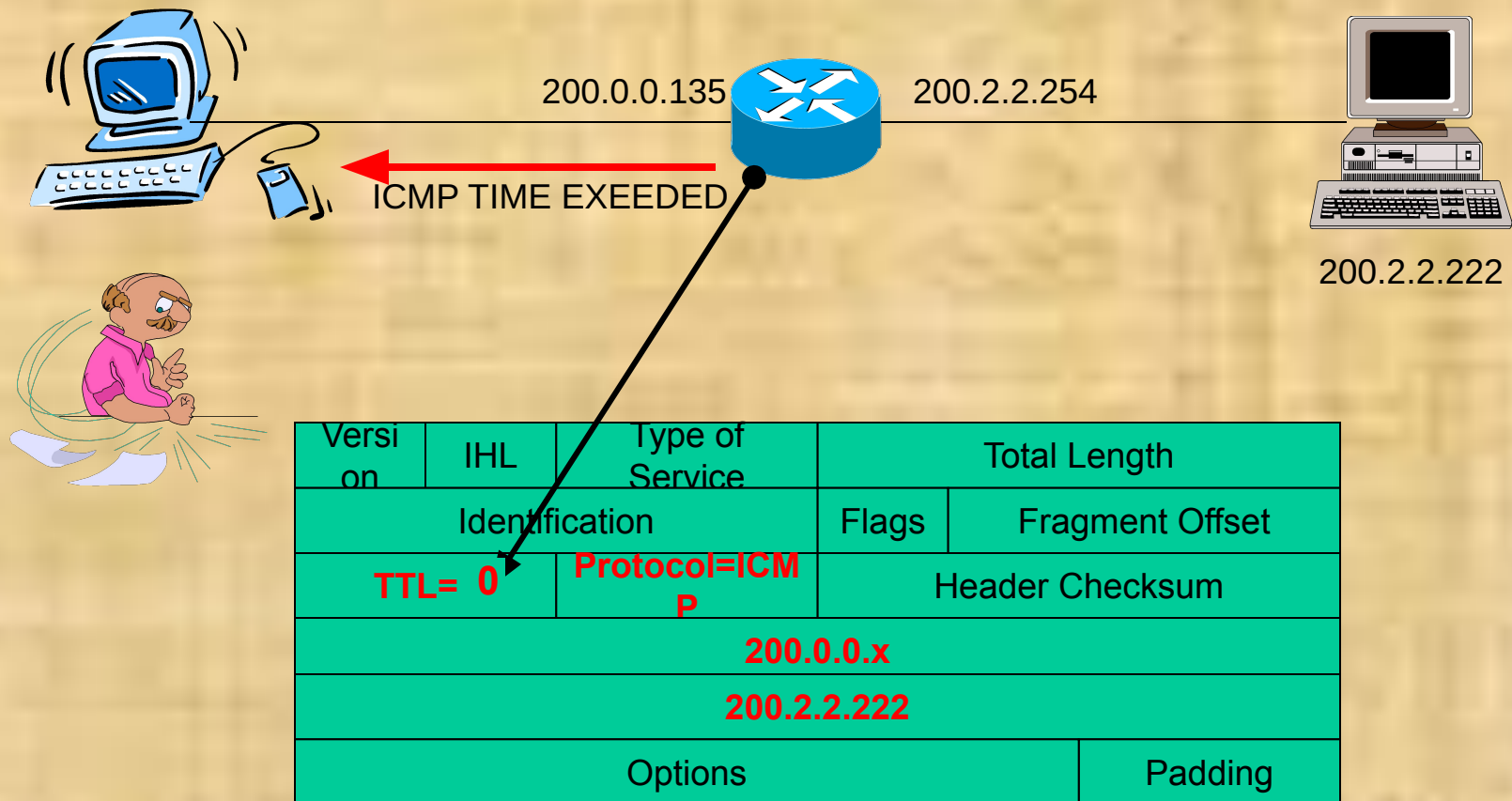
# Отслеживание маршрутов - пример

Windows – утилита **tracert**



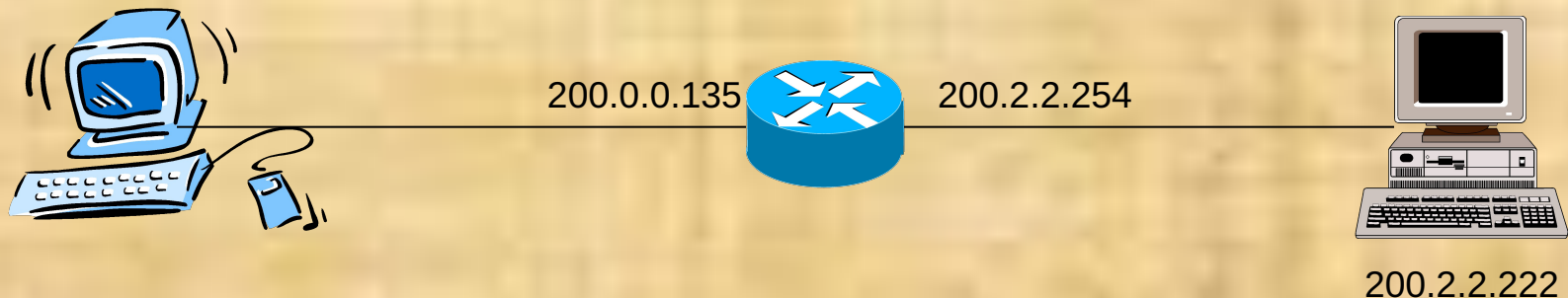
# Отслеживание маршрутов - пример

Windows – утилита **tracert**

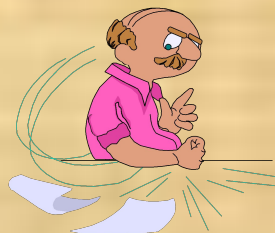


# Отслеживание маршрутов - пример

Windows – утилита **tracert**



ICMP TIME EXCEEDED



Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol=ICMP		Header Checksum	
200.0.0.135				
200.0.0.x				
Options				Padding
ICMP Data				
Отправитель – 200.0.0.x				
Получатель – 200.2.2.222				

# Отслеживание маршрутов - пример

Microsoft Network Monitor - [Capture: 5 (Detail)]

File Edit Display Tools Options Window Help

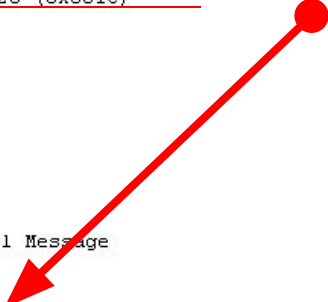
Src MAC...	Protocol	Description	Src Other Addr	Dst Other Addr	Type Other...
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Time Exceeded: 200.2.2.222 (See fram...	200.0.0.135	200.0.0.161	IP
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Time Exceeded: 200.2.2.222 (See fram...	200.0.0.135	200.0.0.161	IP
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Time Exceeded: 200.2.2.222 (See fram...	200.0.0.135	200.0.0.161	IP
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Echo Reply: To 200.00.00.161 From 200...	200.2.2.222	200.0.0.161	IP
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Echo Reply: To 200.00.00.161 From 200...	200.2.2.222	200.0.0.161	IP
.NETRON9...	ICMP	Echo: From 200.00.00.161 To 200.02.02...	200.0.0.161	200.2.2.222	IP
3COM 5...	ICMP	Echo Reply: To 200.00.00.161 From 200...	200.2.2.222	200.0.0.161	IP

ICMP: Time Exceeded: 200.2.2.222 (See frame 9)  
ICMP: Packet Type = Time Exceeded  
ICMP: Time Exceeded Code = Time To Live Exceeded In Transit  
ICMP: Checksum = 0xF4FF  
ICMP: Unused Bytes = 0 (0x0)  
ICMP: Data: Number of data bytes remaining = 28 (0x001C)

ICMP: Description of original IP frame  
ICMP: (IP) Version = 4 (0x4)  
ICMP: (IP) Header Length = 20 (0x14)  
ICMP: (IP) Service Type = 0 (0x0)  
ICMP: (IP) Total Length = 92 (0x5C)  
ICMP: (IP) Identification = 32901 (0x8085)  
ICMP: (IP) Flags Summary = 0 (0x0)  
ICMP: (IP) Fragment Offset = 0 (0x0) bytes  
ICMP: (IP) Time to Live = 1 (0x1)  
ICMP: (IP) Protocol = ICMP - Internet Control Message  
ICMP: (IP) Checksum = 0xA59A  
ICMP: (IP) Source Address = 200.0.0.161  
ICMP: (IP) Destination Address = 200.2.2.222  
ICMP: (IP) Data: Number of data bytes remaining = 8 (0x0008)

ICMP: Description of original ICMP frame  
ICMP: Checksum = 0x74FF  
ICMP: Identifier = 512 (0x200)  
ICMP: Sequence Number = 33024 (0x8100)

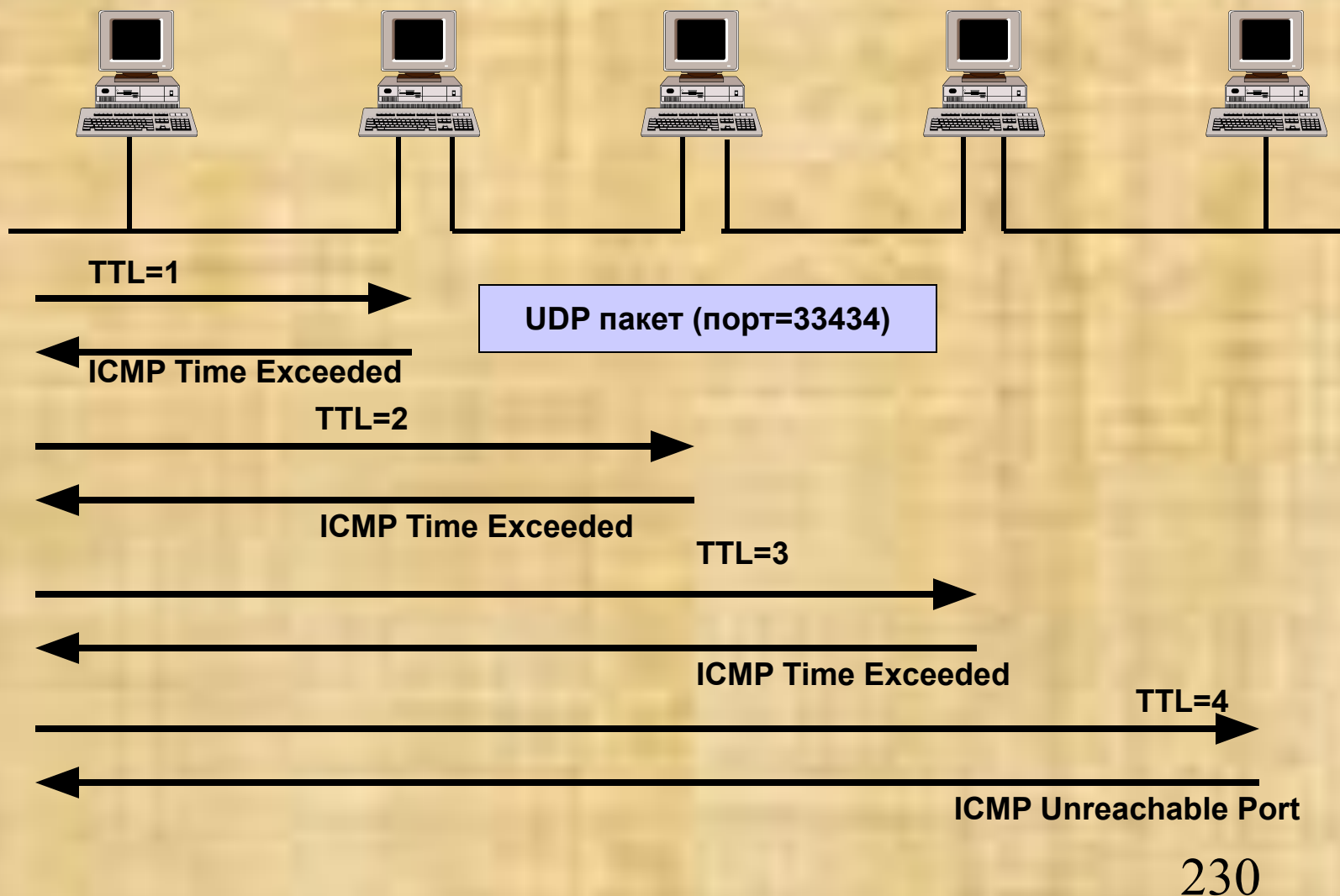
Адрес объекта атаки



# Отслеживание маршрутов (UDP+ICMP)

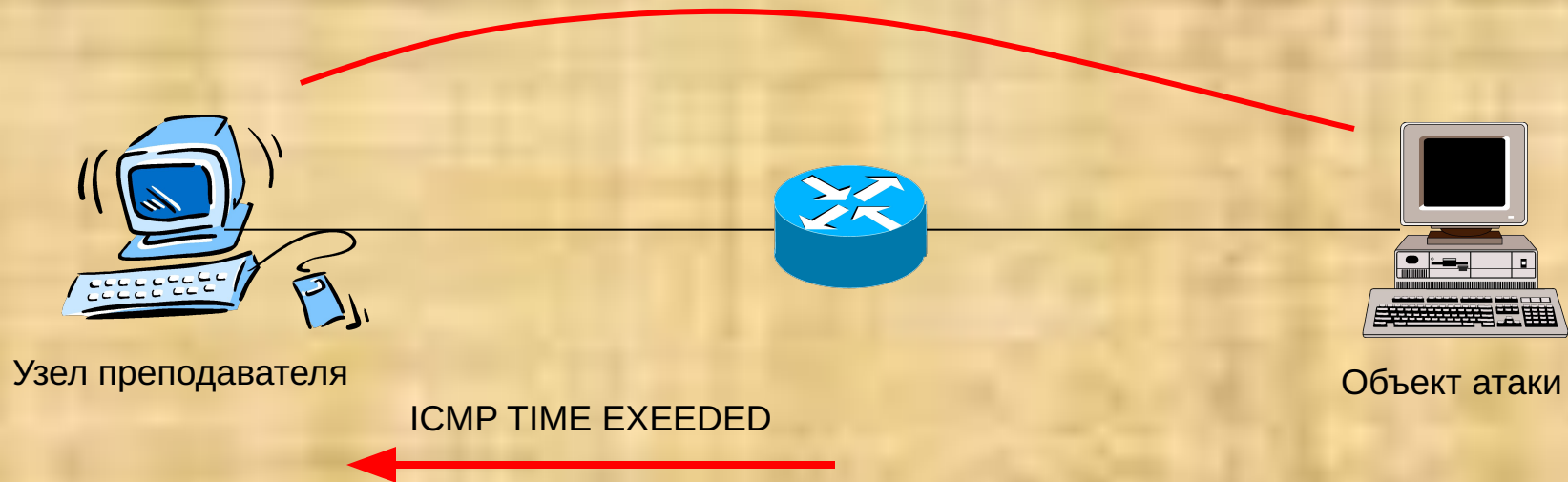
```
# traceroute edward
```

edward





## Практическая работа 4



Определить с помощью сетевого анализатора адрес объекта атаки по сообщению ICMP\_TIME\_EXCEEDED