

Протокол IP

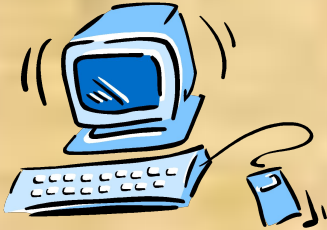
Сетевой уровень в стеке TCP/IP

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

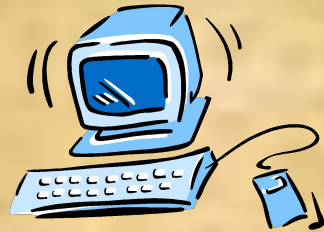
TELNET, FTP, DNS, другие
TCP, UDP
IP, ICMP

Идентификация узлов

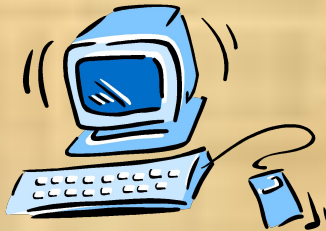
IP-адрес



IP-адрес



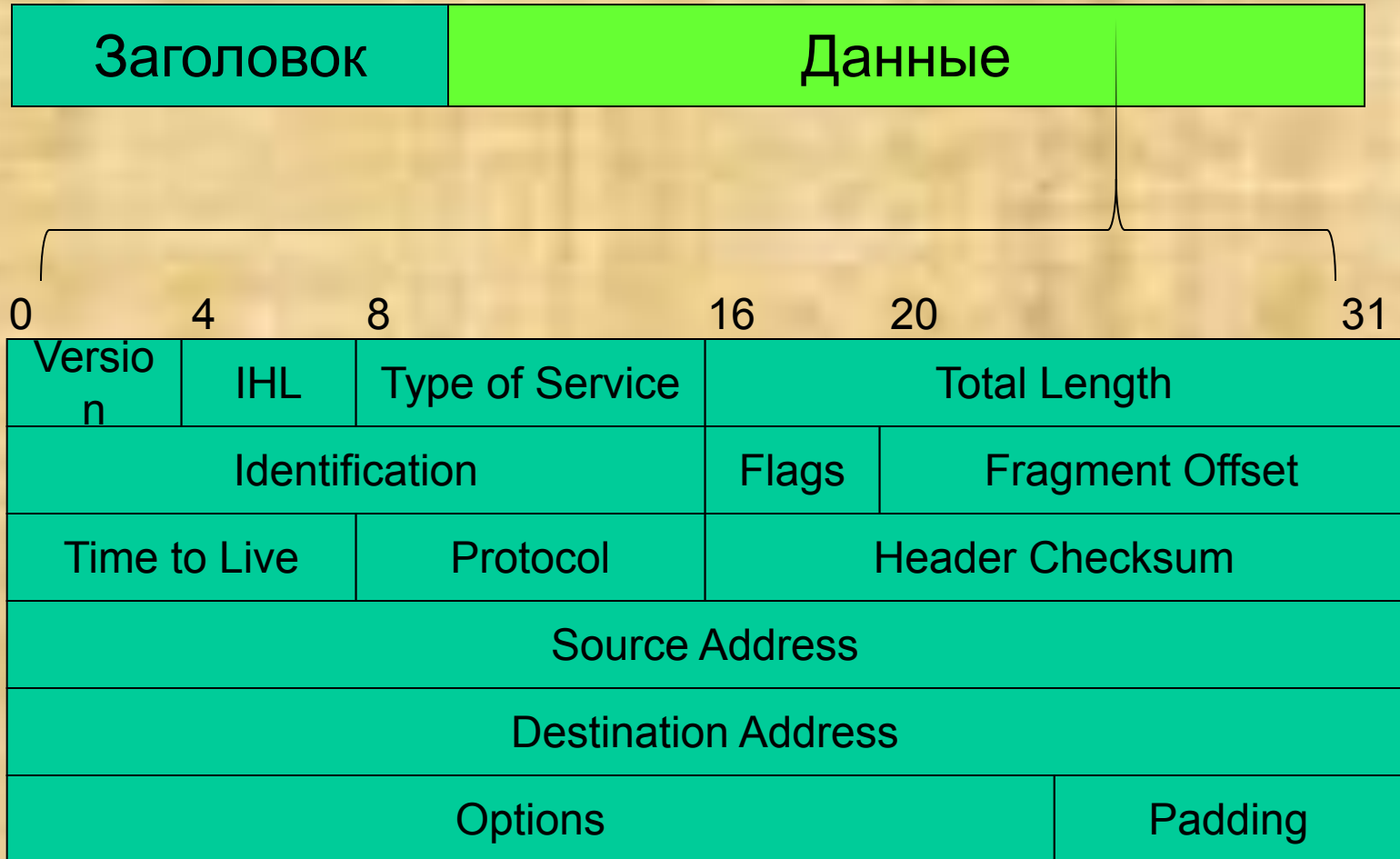
IP-адрес



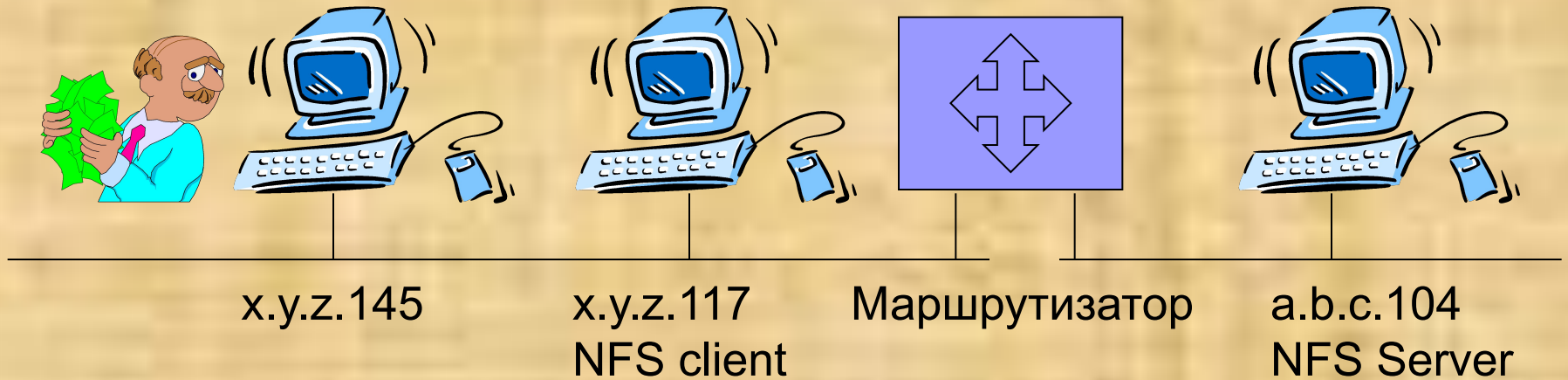
IP-адрес



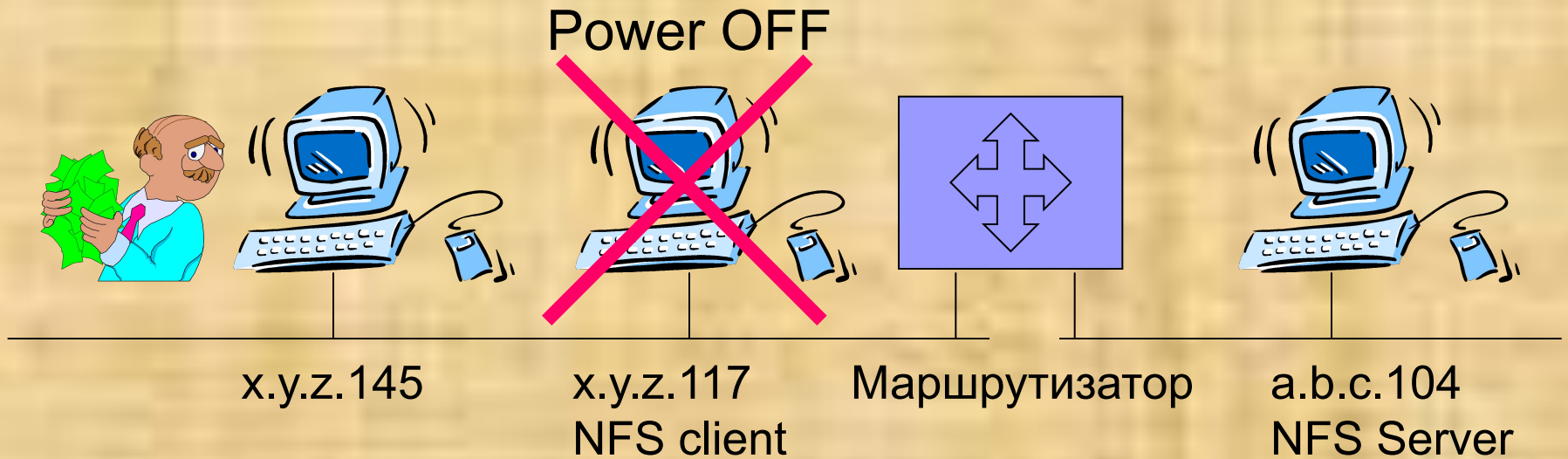
Формат заголовка IP-пакета



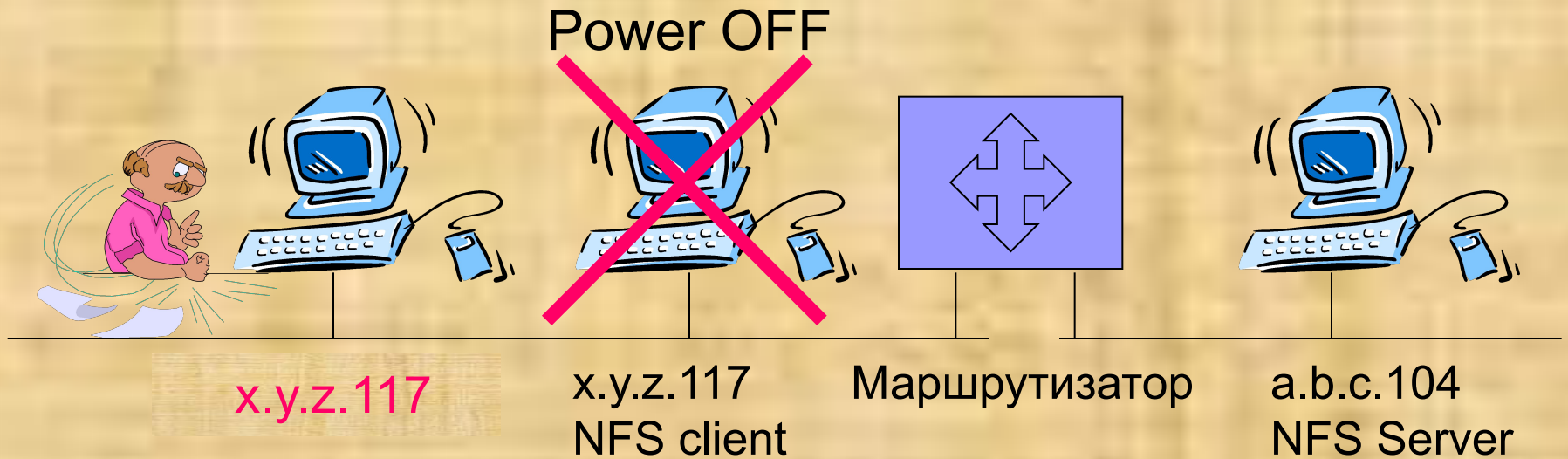
Атака Address Masquerading



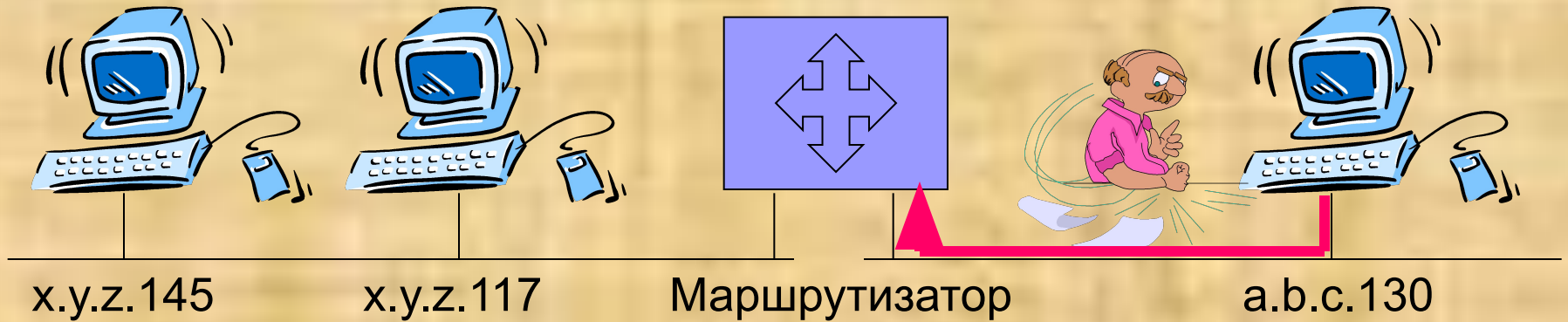
Атака Address Masquerading



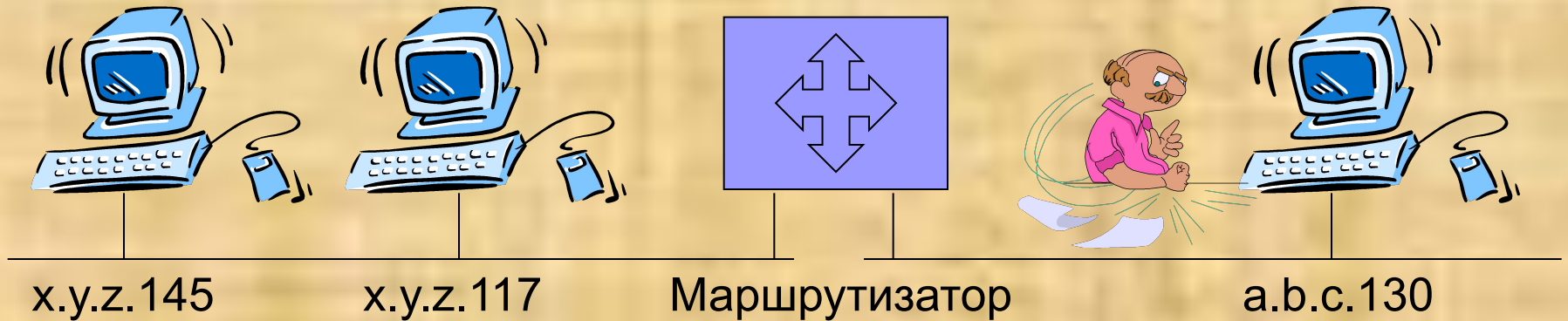
Атака Address Masquerading



Address Spoofing

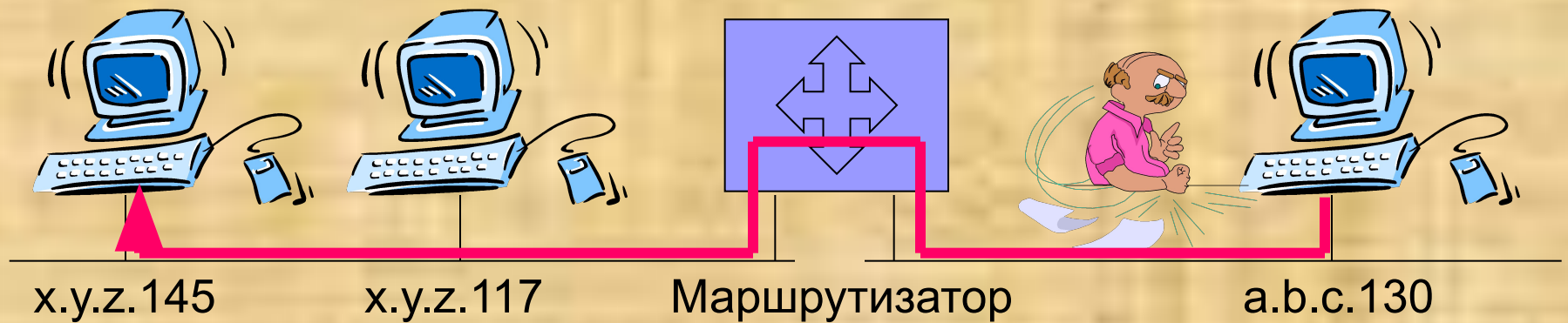


Address Spoofing

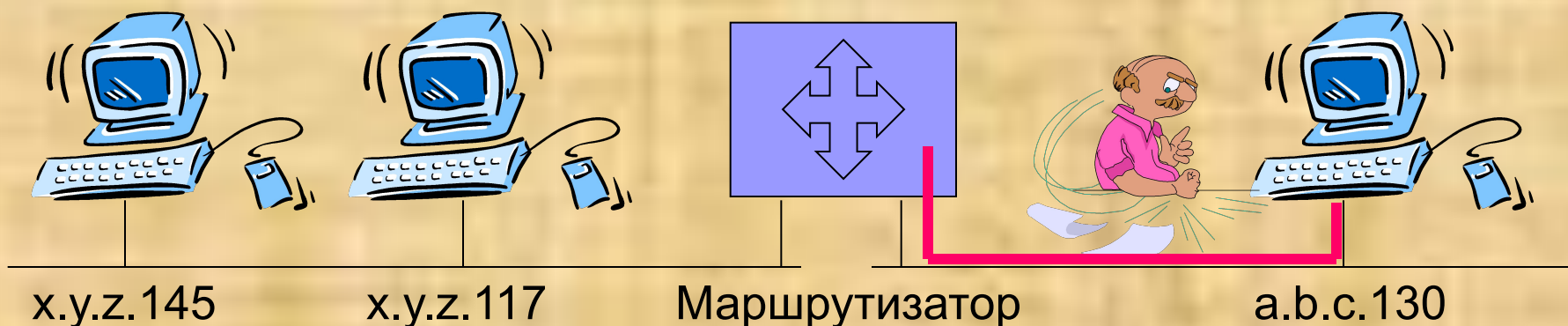


Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
x.y.z.120				
x.y.z.145				
Options				Padding

Address Spoofing (IPspoofing)

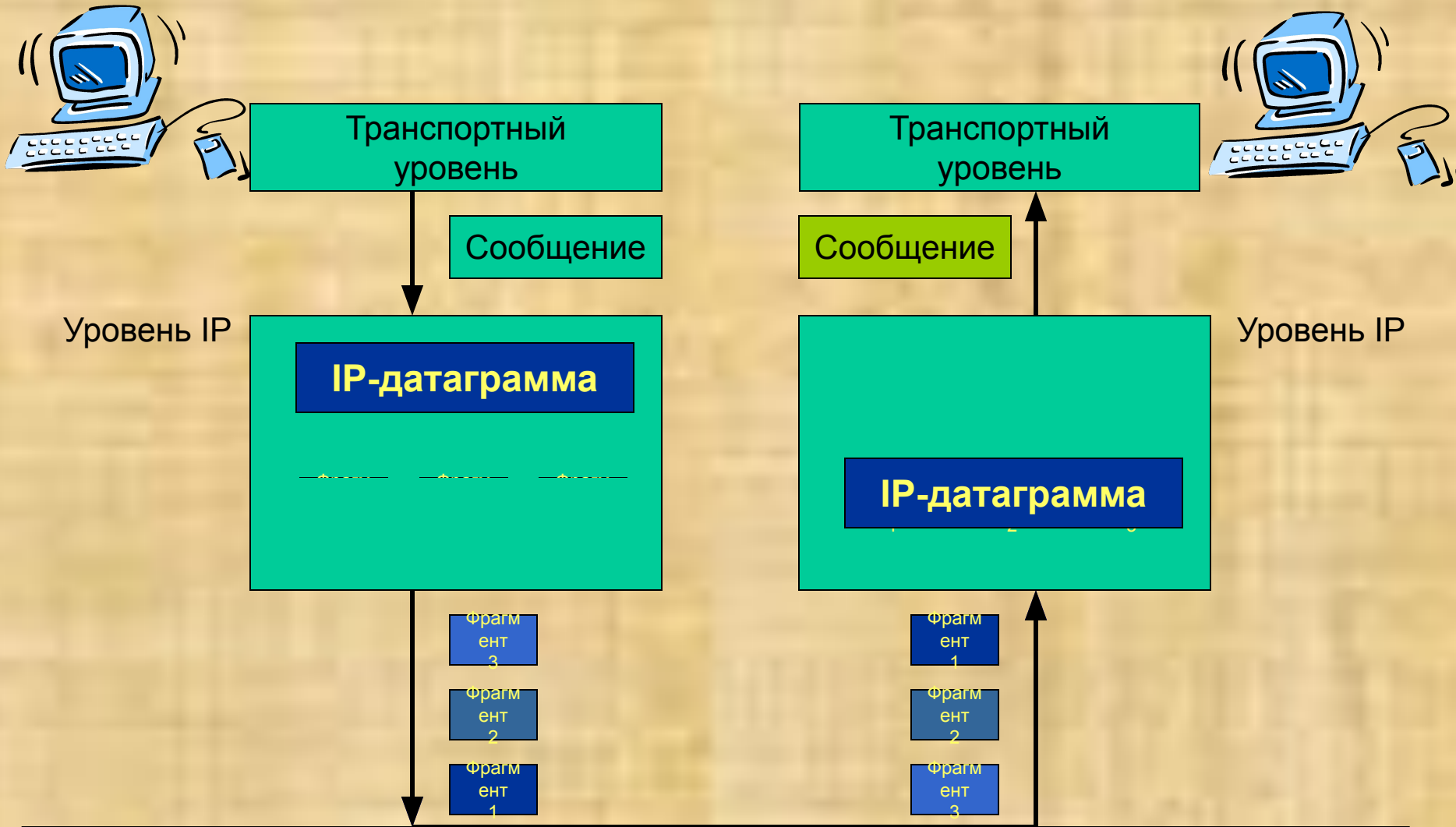


Адреса источника, подлежащие фильтрации

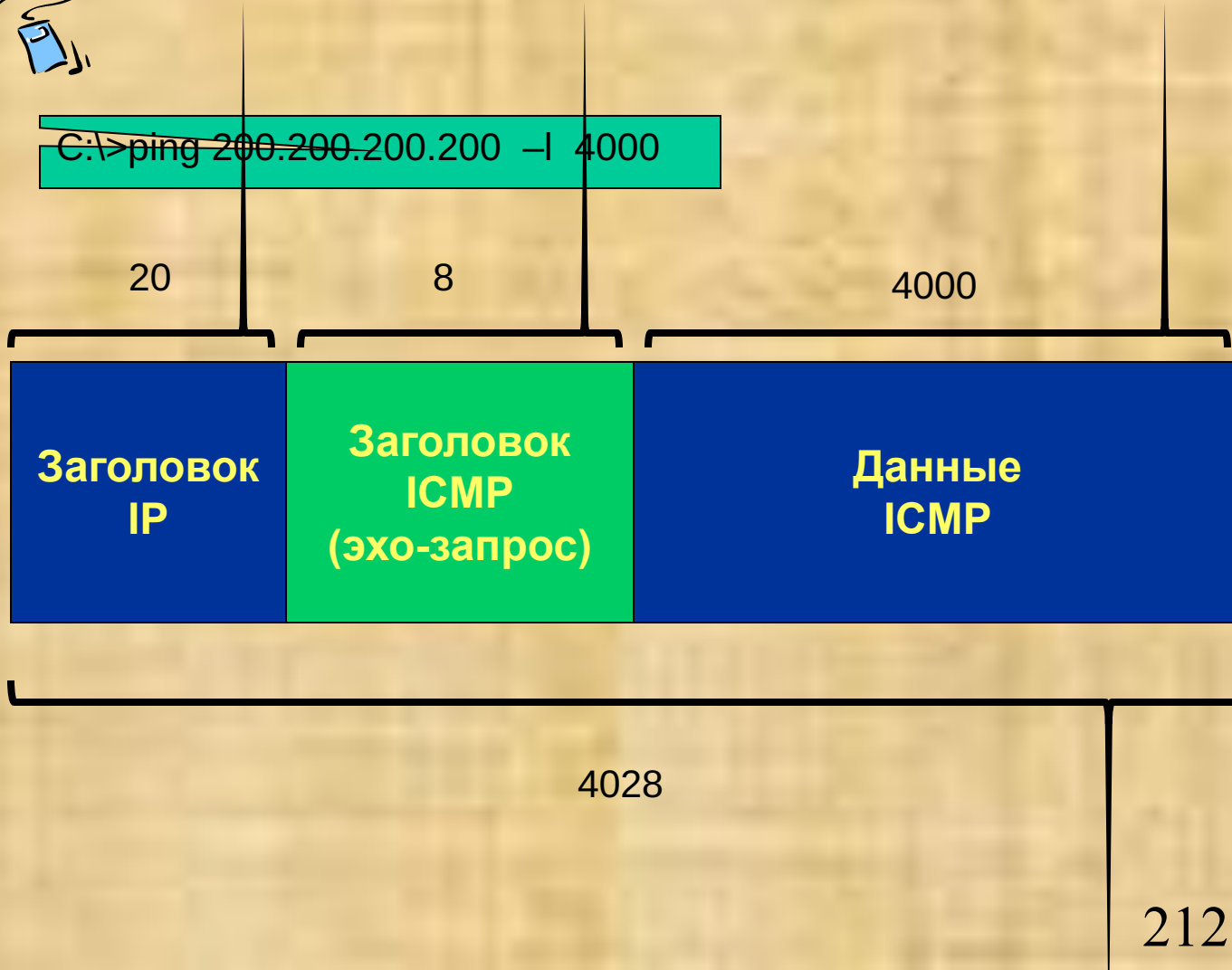
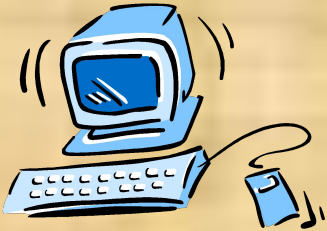


1. Адрес данного узла
2. Адреса, рекомендуемые для внутренних сетей
3. Адреса для группового вещания (224.0.0.0 – 239.255.255.255)
4. Адреса класса E (240.0.0.0 – 247.255.255.255)
5. Адреса типа «обратная петля» 127.x.x.x
6. Некорректные адреса (например, 0.0.0.0)

Фрагментация



Фрагментация



Фрагментация

20

8

4000



Первый
фрагмент

20

8

1472



Второй
фрагмент

20

1500

1480



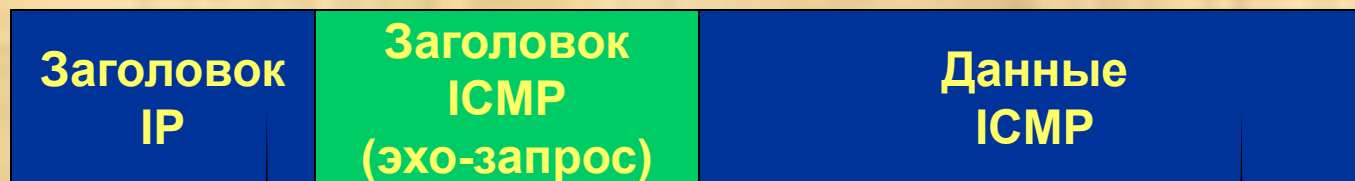
Фрагментация

20

8

1472

Первый
фрагмент



Второй
фрагмент

1500

20

1480



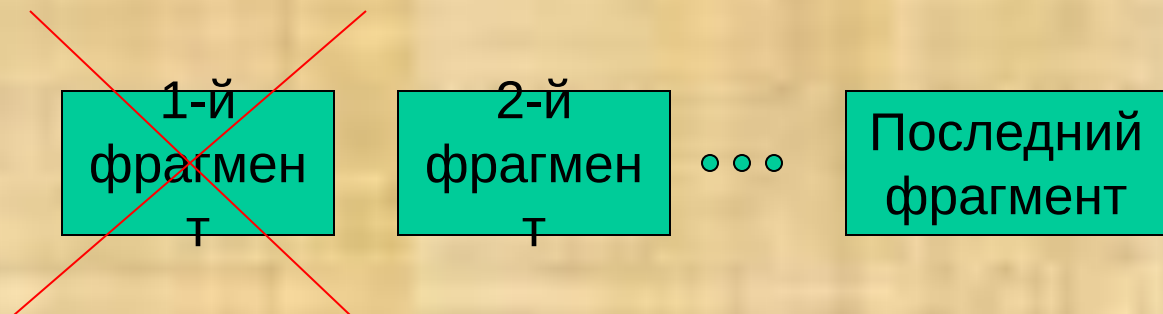
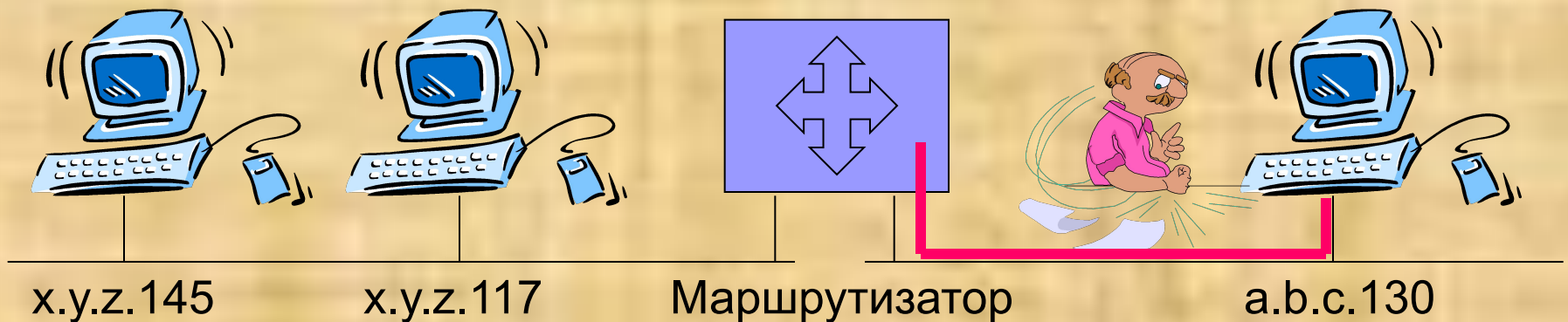
Последний
фрагмент

20

1048



Фрагментация с целью обхода фильтрации



Фрагментация с целью обхода фильтрации

The screenshot displays the Network Monitor application interface. At the top, the title bar reads "Network Monitor" with standard window controls. The menu bar includes "File", "Edit", "Display", "Tools", "Options", "Window", and "Help". Below the menu is a toolbar with various icons for file operations and network management.

The main window is divided into several panes. The top-left pane, titled "\Ethernet\NET1 Capture Window (Station Stats)", shows network utilization metrics. It includes a "% Network Utilization" gauge (0 to 100) and a "Frames Per Second" gauge (0 to 100). The "Frames Per Second" gauge shows a value of 7. To the right of this pane, the "Time Elapsed" is 00:00:23.532, and the "Network Statistics" section lists: # Frames: 23, # Broadcasts: 4, # Multicasts: 0, # Bytes: 17414, and # Frames Dropped: 0.

The bottom pane, titled "Capture: 1 (Summary)", displays a table of captured packets. The table has columns for Time, Src MAC Addr, Dst MAC Addr, Protocol, and Description. The data shows a series of ICMP Echo and Echo Reply packets between ISS140 and EDU-MAIN2K, with IP fragmentation details.

Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Sta
00.261	ISS140	EDU-MAIN2K	ICMP	Echo, From 200.01.01.15 To 200.01.01.254	IS
00.261	ISS140	EDU-MAIN2K	IP	ID = 0x8408; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	IS
00.264	EDU-MAIN2K	ISS140	ICMP	Echo Reply, To 200.01.01.15 From 200.01.01.254	EI
00.264	EDU-MAIN2K	ISS140	IP	ID = 0x2A84; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	EI
01.259	ISS140	EDU-MAIN2K	ICMP	Echo, From 200.01.01.15 To 200.01.01.254	IS
01.259	ISS140	EDU-MAIN2K	IP	ID = 0x8508; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	IS
01.262	EDU-MAIN2K	ISS140	ICMP	Echo Reply, To 200.01.01.15 From 200.01.01.254	EI
01.263	EDU-MAIN2K	ISS140	IP	ID = 0x2A85; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	EI
02.261	ISS140	EDU-MAIN2K	ICMP	Echo, From 200.01.01.15 To 200.01.01.254	IS
02.261	ISS140	EDU-MAIN2K	IP	ID = 0x8608; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	IS
02.264	EDU-MAIN2K	ISS140	ICMP	Echo Reply, To 200.01.01.15 From 200.01.01.254	EI
02.264	EDU-MAIN2K	ISS140	IP	ID = 0x2A86; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	EI
03.262	ISS140	EDU-MAIN2K	ICMP	Echo, From 200.01.01.15 To 200.01.01.254	IS
03.262	ISS140	EDU-MAIN2K	IP	ID = 0x8708; Proto = ICMP; Len: 548, Frag. Offset = 1480 (0x5C8)	IS
03.265	EDU-MAIN2K	ISS140	ICMP	Echo Reply, To 200.01.01.15 From 200.01.01.254	EI

At the bottom of the window, a status bar shows "TCP protocol summary", "F#: 7/24", "Off: 34 (x22)", and "L: 20 (x14)".

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

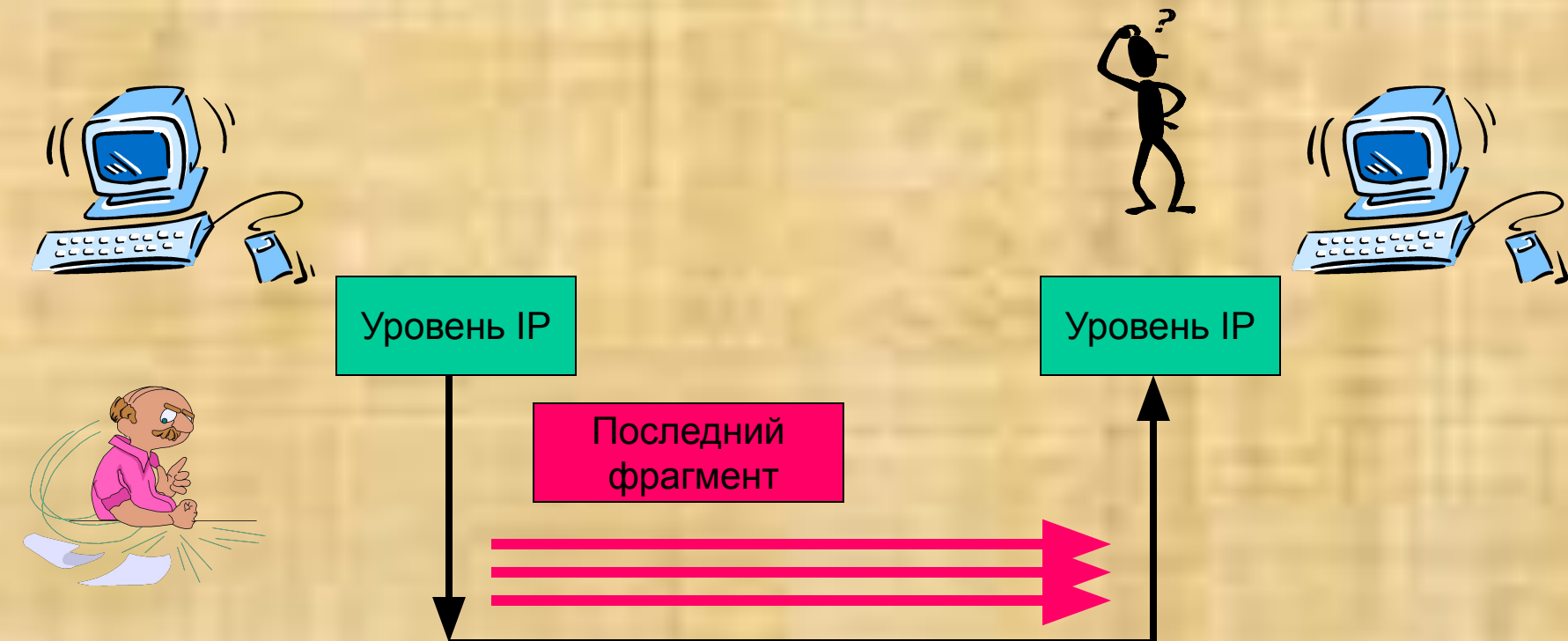
Заголовок 2-го фрагмента

Ver	IHL	ToS	Total Length=216	
333		0	240	

Данные=196 байт

есть следующий
фрагмент

Ошибки реализации функции фрагментации

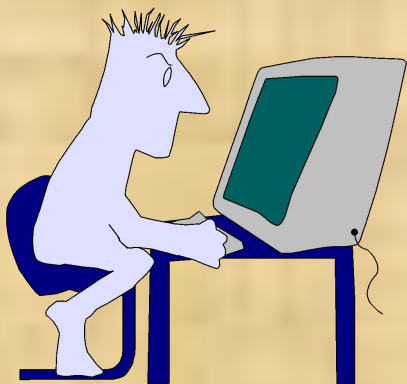


Атака IP DoS Fragmenting (jolt2)

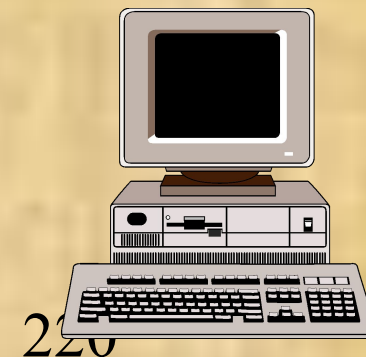
Атака Ping of Death

Тип=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

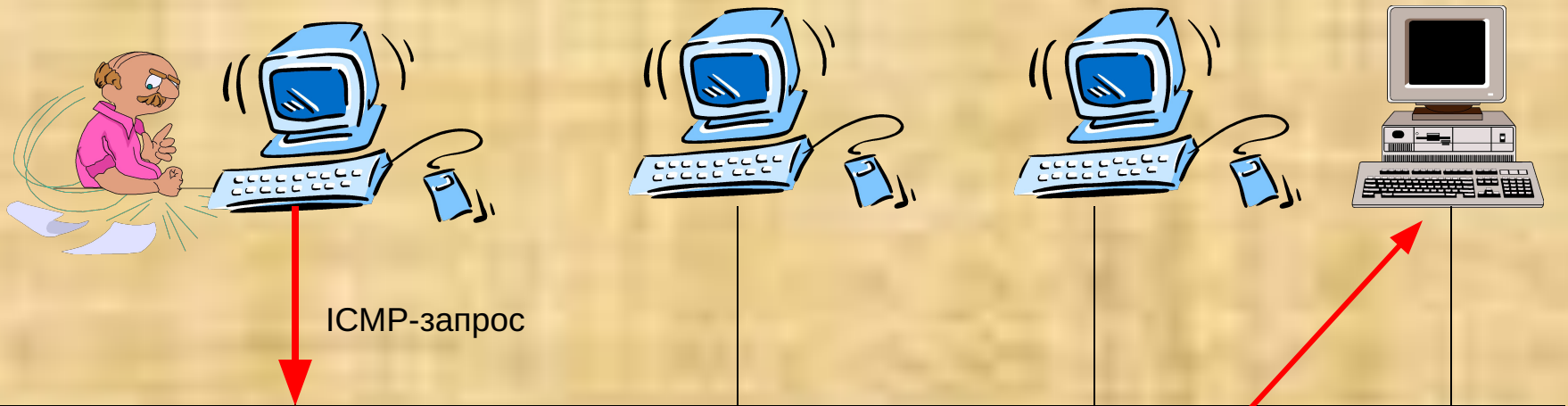
ICMP Subnet Mask Address Request

ICMP Redirect

ICMP Timestamp

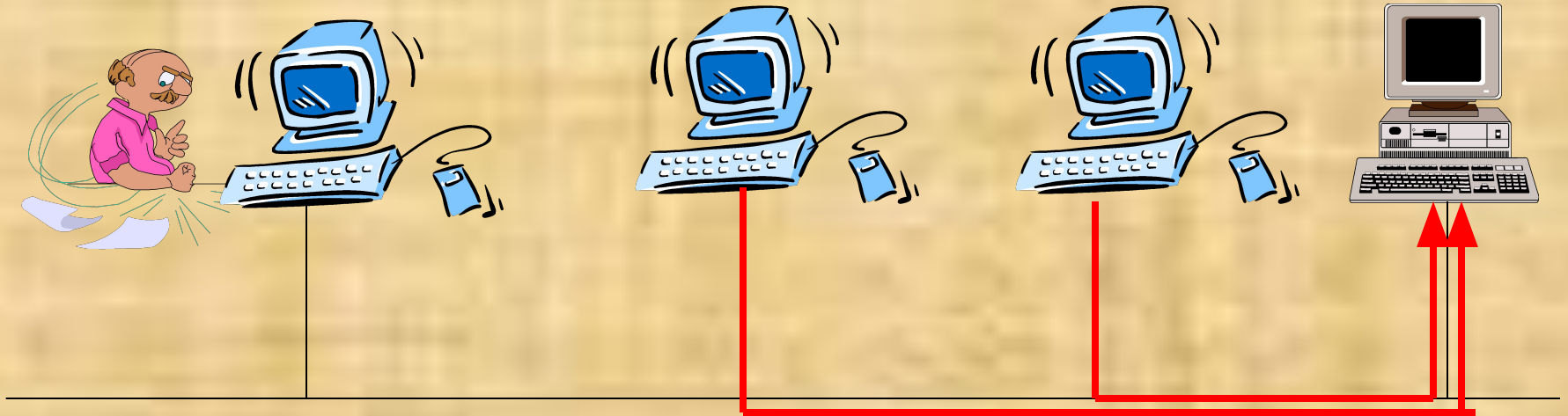
Smurf

Атака Smurf



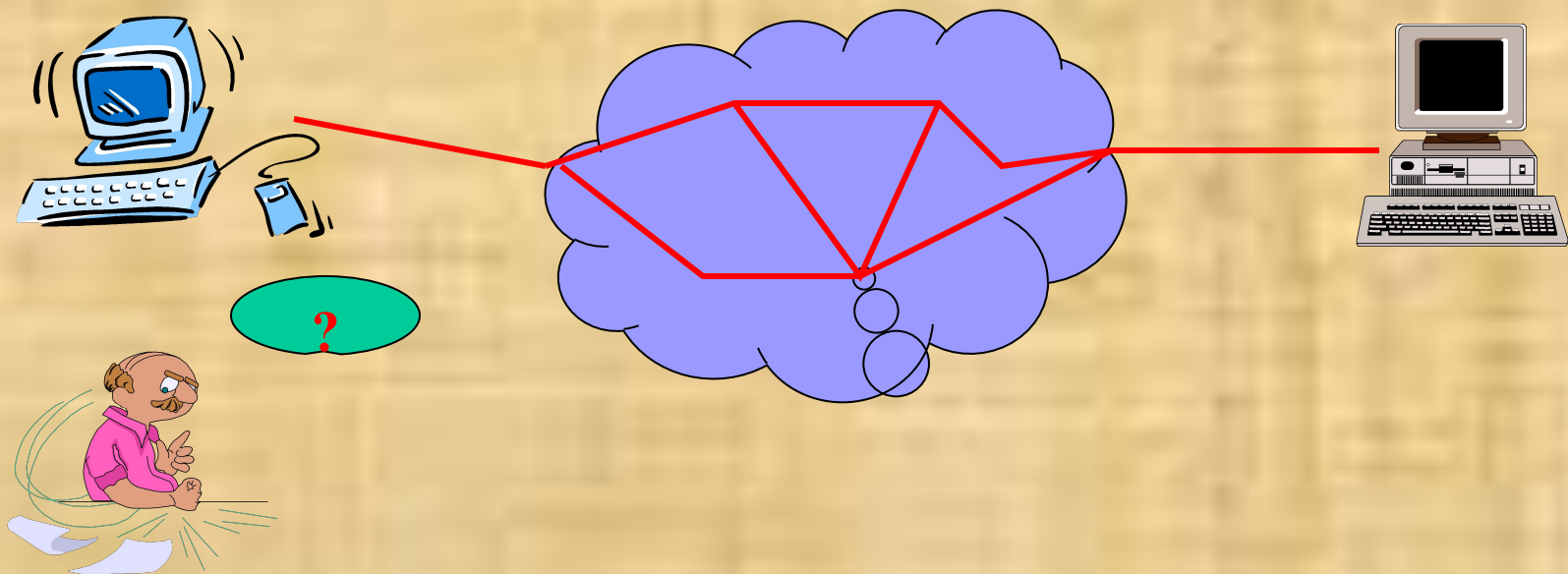
Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
TTL	Protocol=ICMP		Header Checksum	
Адрес объекта атаки				
Адрес сети или широковещательный				
Options			Padding	

Атака Smurf



ICMP-ответы от всех узлов сегмента

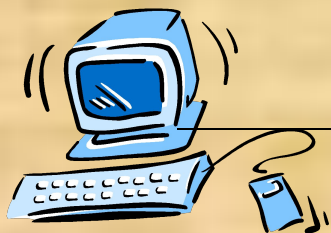
Отслеживание маршрутов



- Протокол ICMP
- Протокол UDP

Отслеживание маршрутов - пример

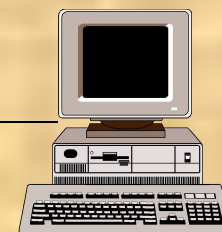
Windows – утилита **tracert**



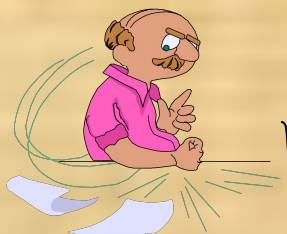
200.0.0.135



200.2.2.254



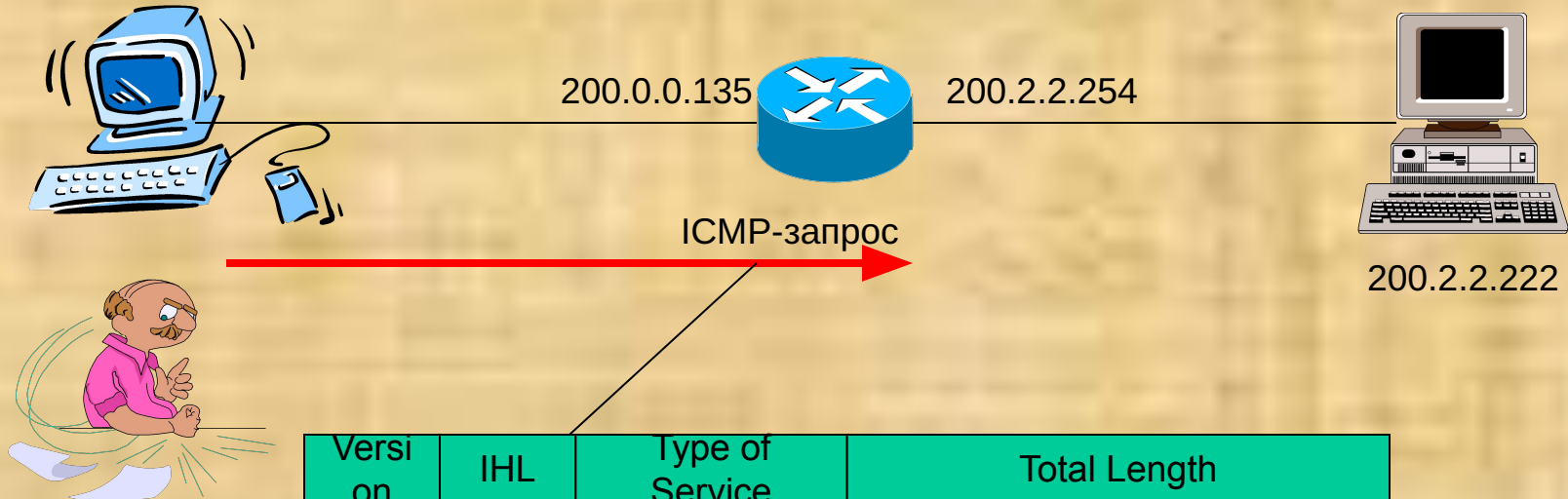
200.2.2.222



```
C:\> tracert 200.2.2.222 -d
```

Отслеживание маршрутов - пример

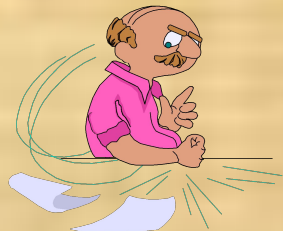
Windows – утилита **tracert**



Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
TTL=1		Protocol=ICMP	Header Checksum	
200.0.0.x				
200.2.2.222				
Options			Padding	

Отслеживание маршрутов - пример

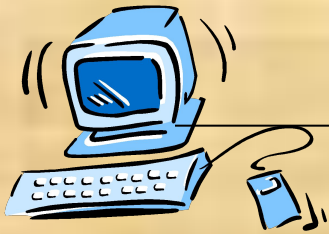
Windows – утилита **tracert**



Version		Type of Service	Total Length	
Identification		Flags	Fragment Offset	
TTL= 0	Protocol=ICMP	Header Checksum		
200.0.0.x				
200.2.2.222				
Options			Padding	

Отслеживание маршрутов - пример

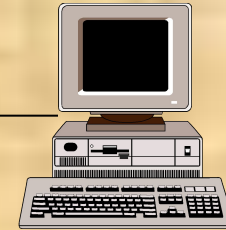
Windows – утилита **tracert**



200.0.0.135

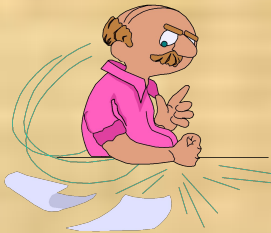


200.2.2.254



200.2.2.222

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)

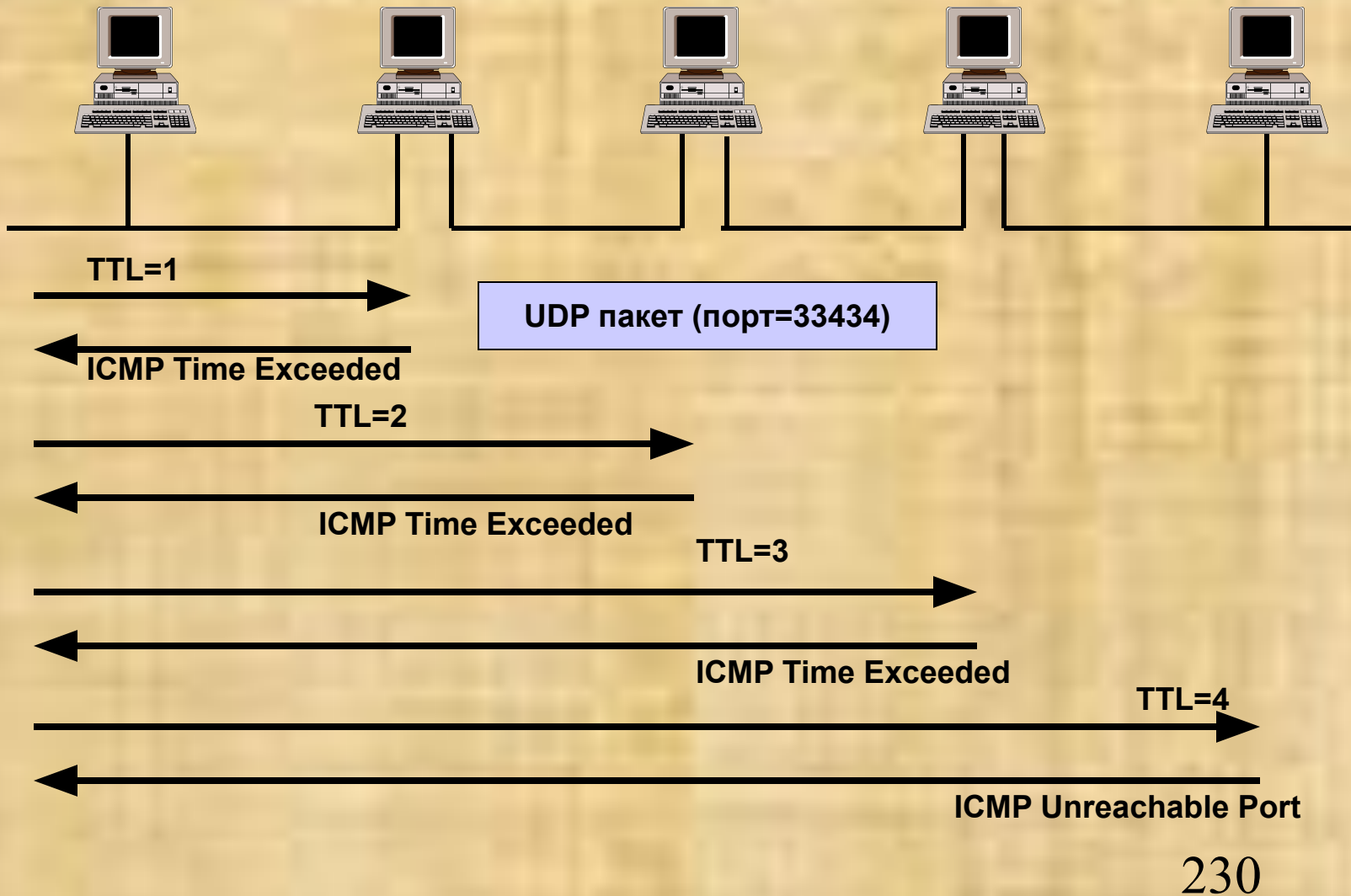
Summary of the IP packet F#: 10/22 Off: 14 (xE) L: 20 (x14)

Адрес объекта атаки

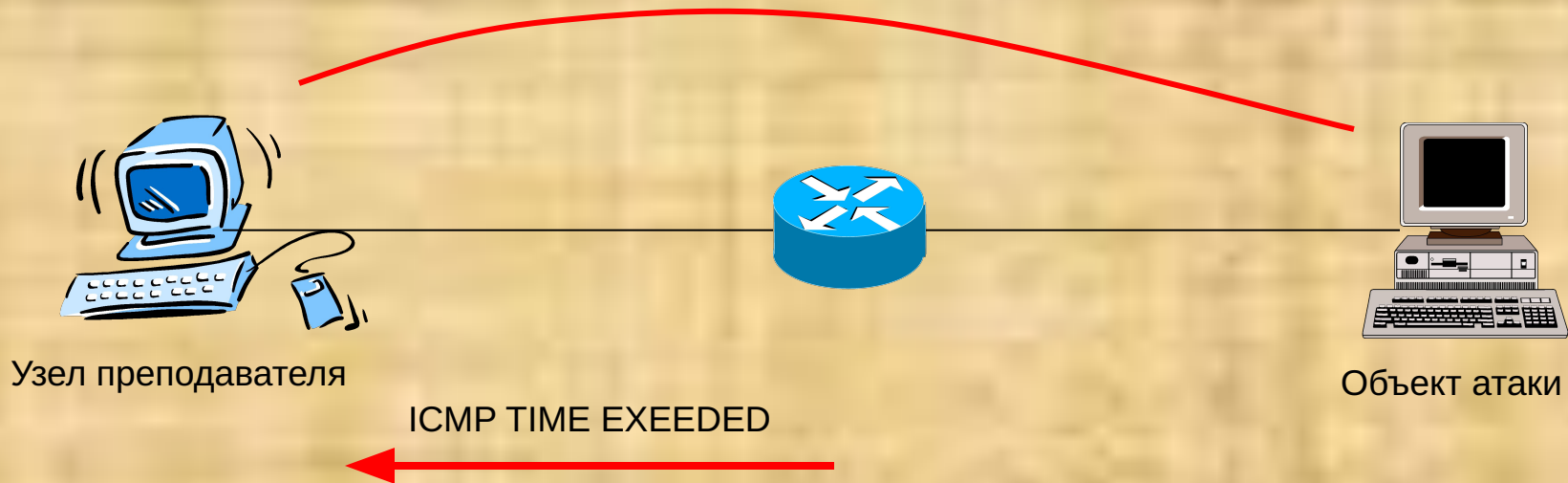
Отслеживание маршрутов (UDP+ICMP)

```
# traceroute edward
```

edward



Практическая работа 4



Определить с помощью сетевого анализатора адрес объекта атаки по сообщению ICMP_TIME_EXCEEDED