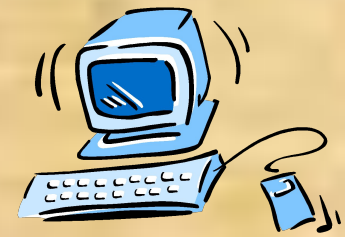
Протокол IP

Сетевой уровень в стеке TCP/IP

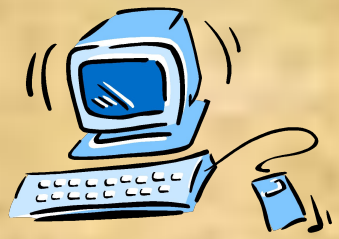
7	Уровень приложения	TELNET, FTP, DNS, другие
6	Уровень представления	
5	Уровень соединения	
4	Транспортный уровень	TCP, UDP
3	Сетевой уровень	IP, ICMP
2	Канальный уровень	
1	Физический уровень	

Идентификация узлов

IP-адрес

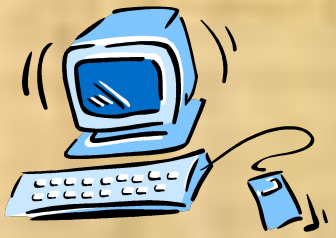


IP-адрес

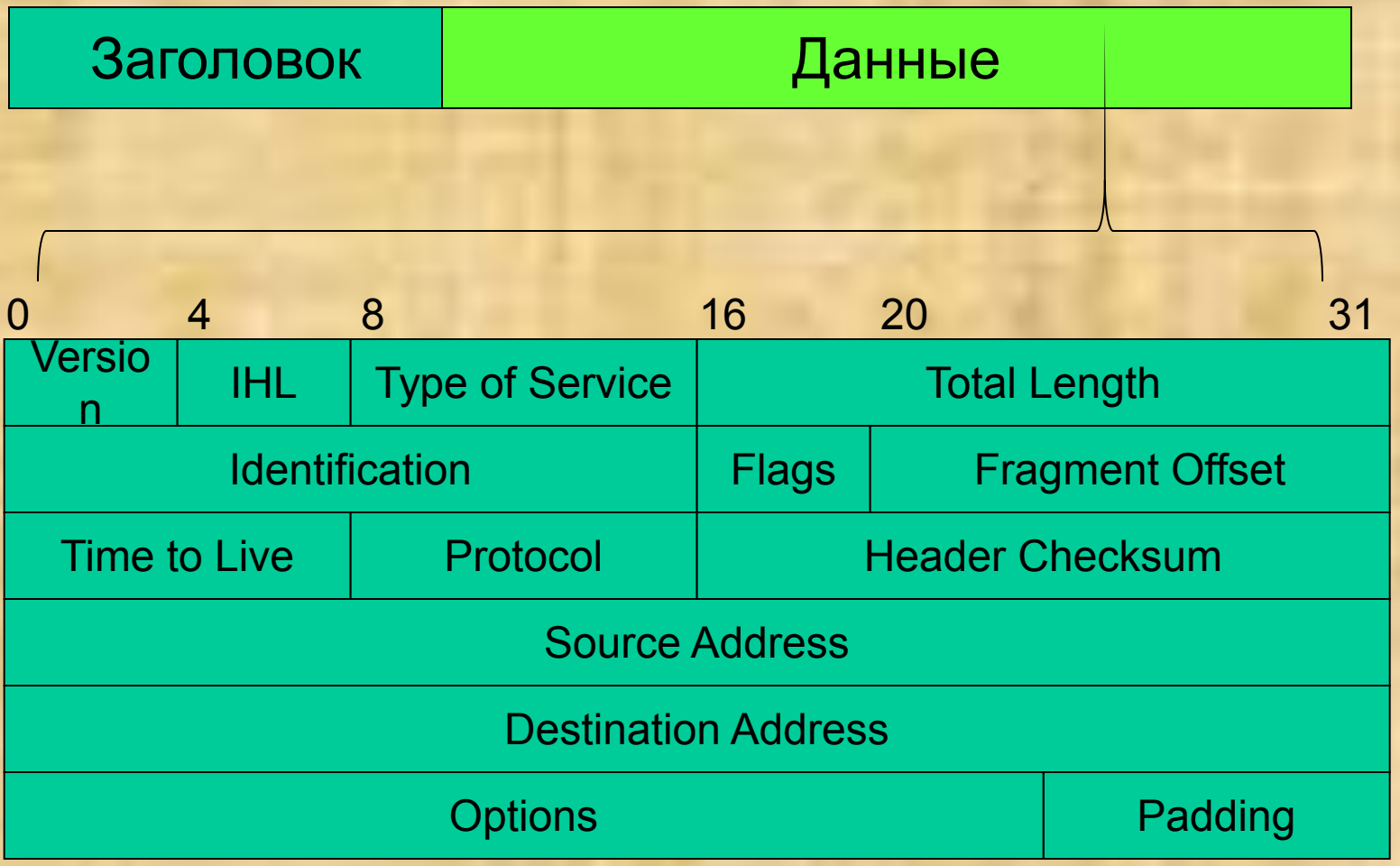


IP-адрес

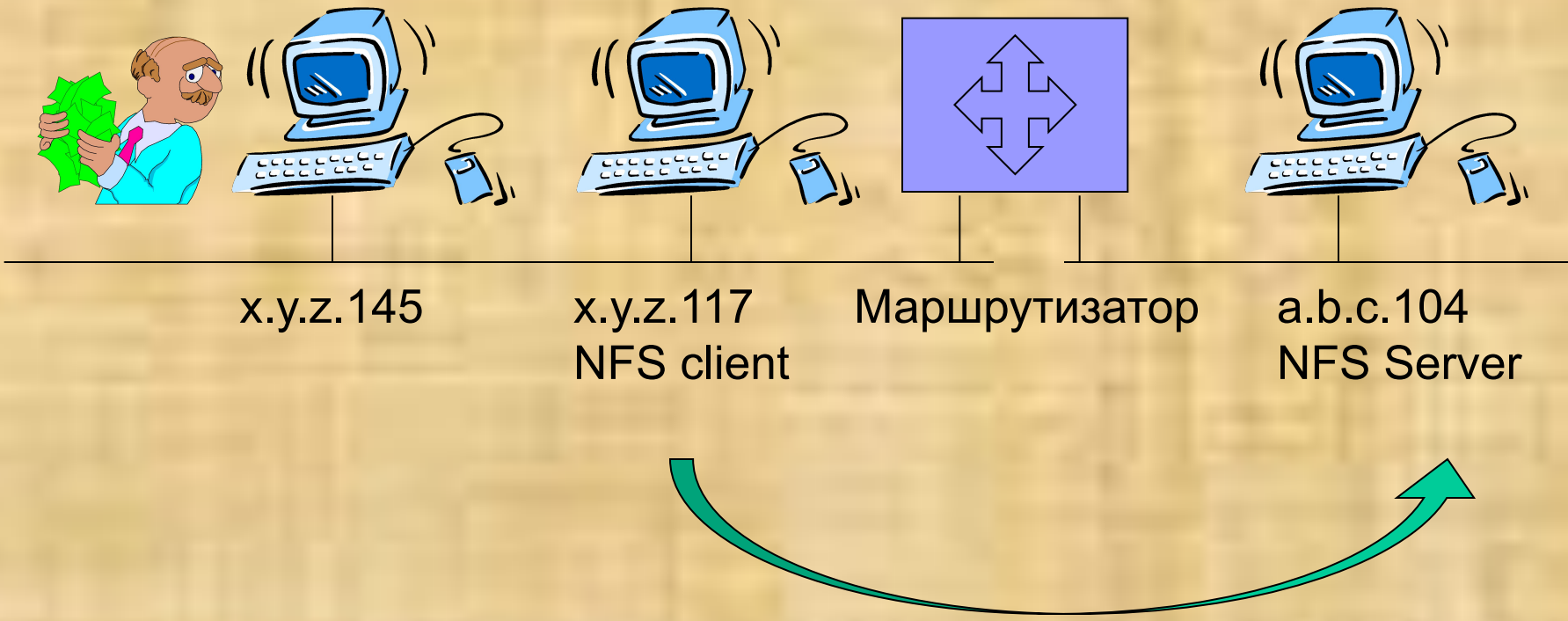
IP-адрес



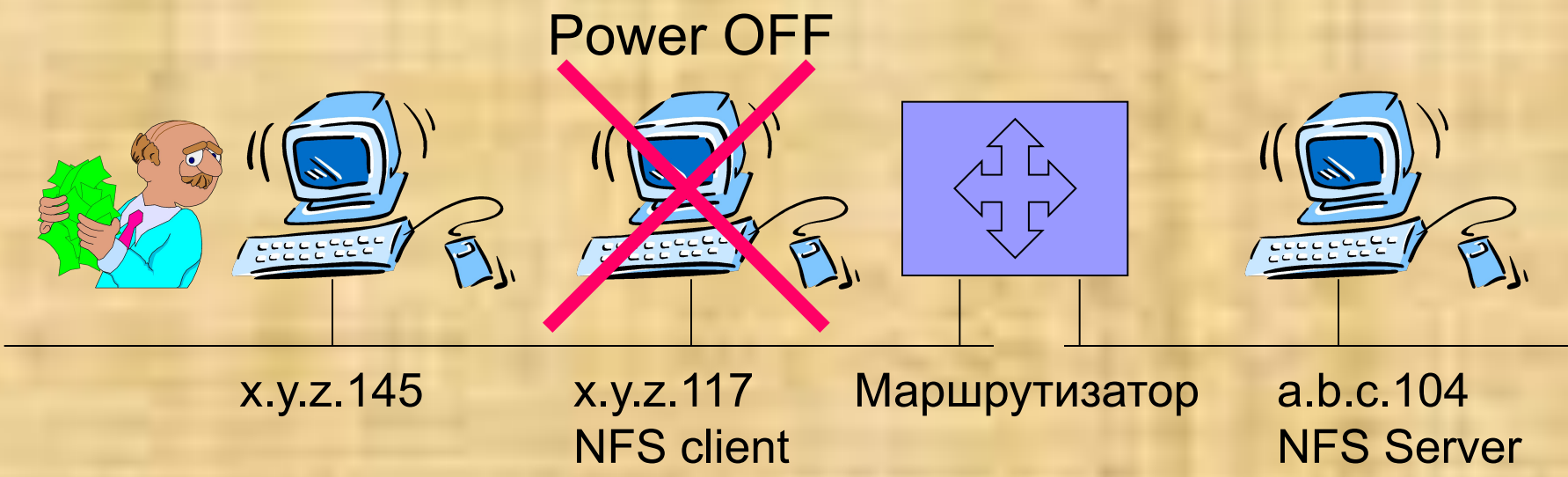
Формат заголовка IP-пакета



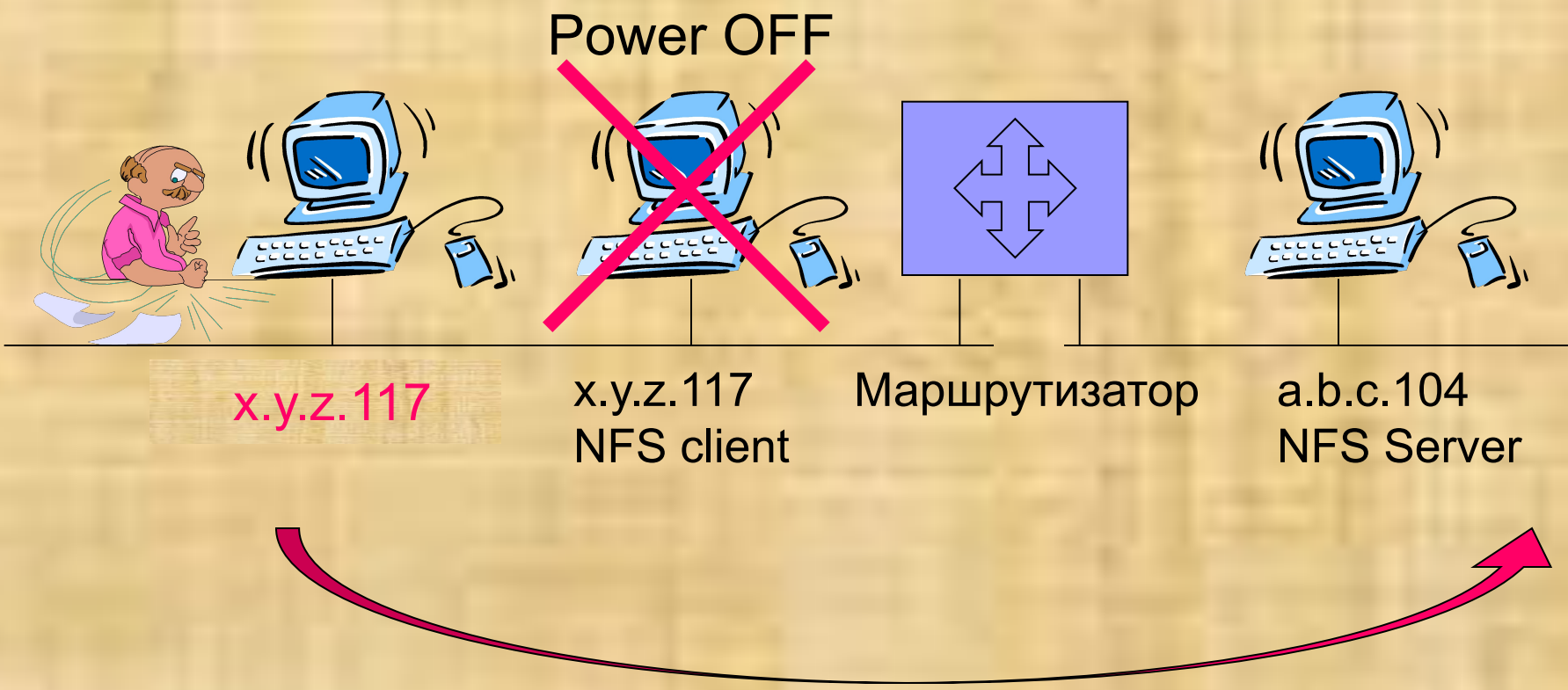
Атака Address Masquerading



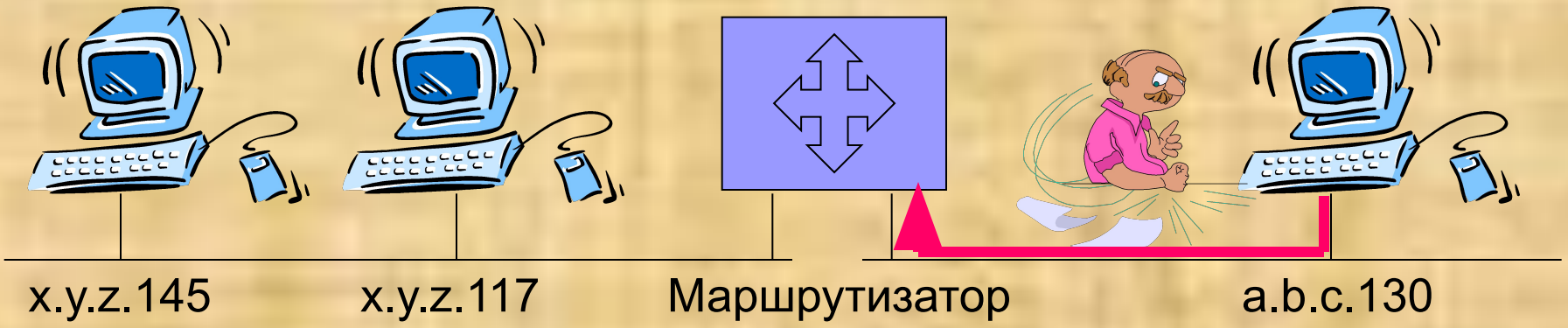
Атака Address Masquerading



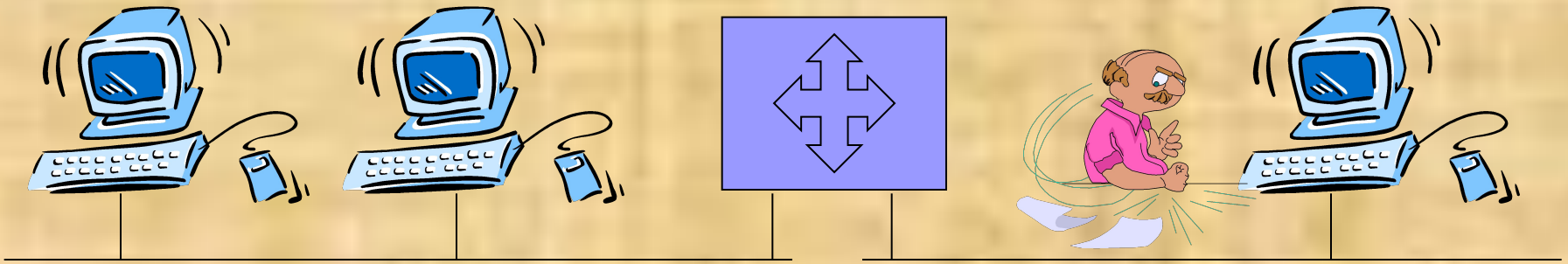
Атака Address Masquerading



Address Spoofing

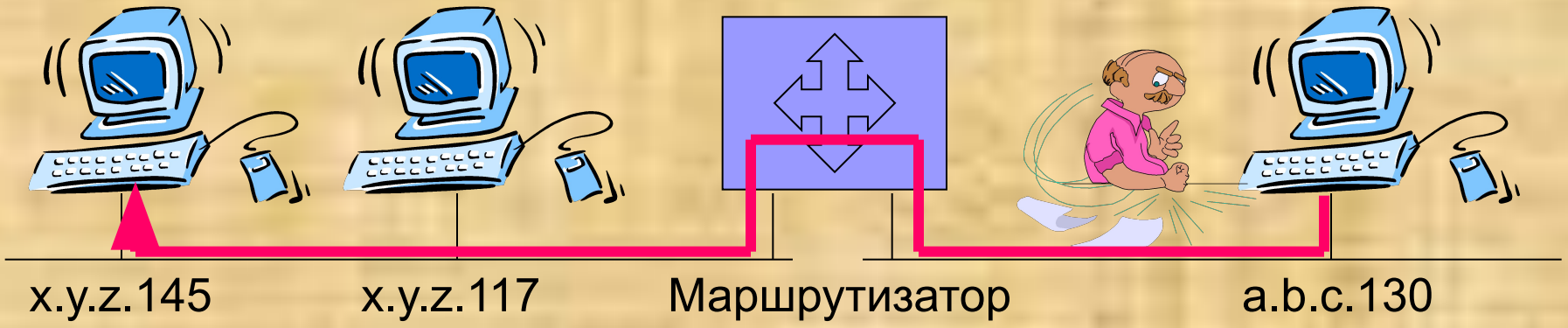


Address Spoofing

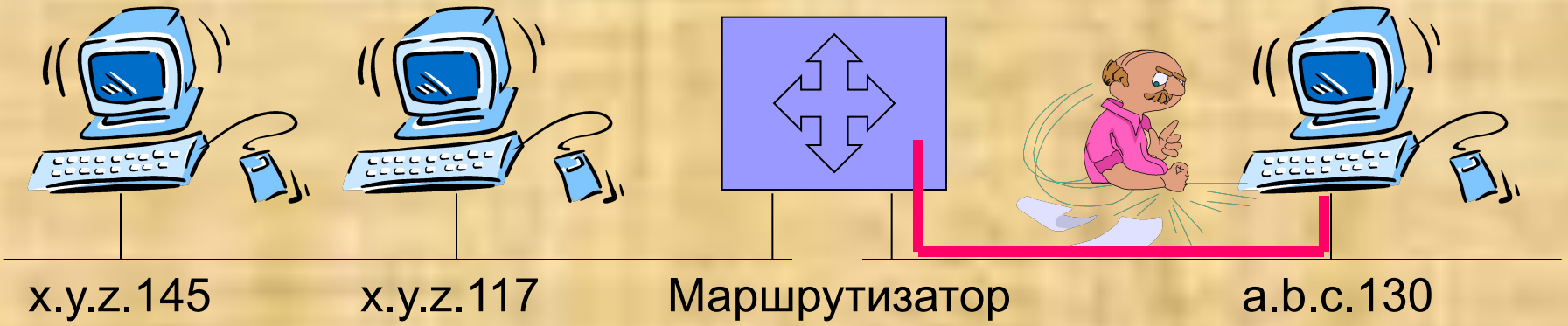


Versi on	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
x.y.z.120				
x.y.z.145				
Options				Padding

Address Spoofing (IPSpoofing)

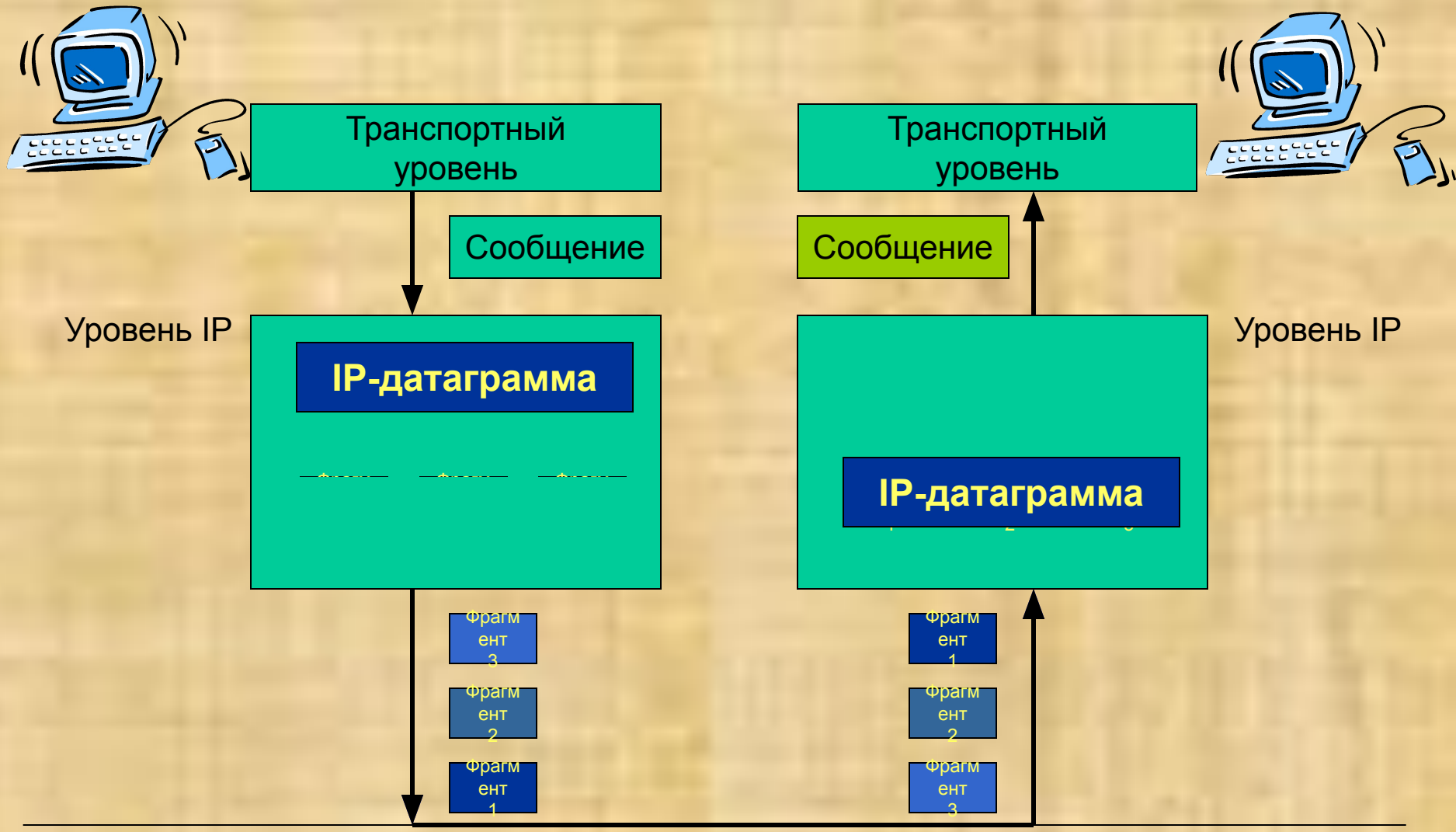


Адреса источника, подлежащие фильтрации

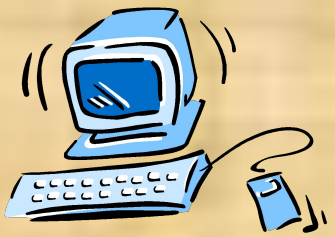


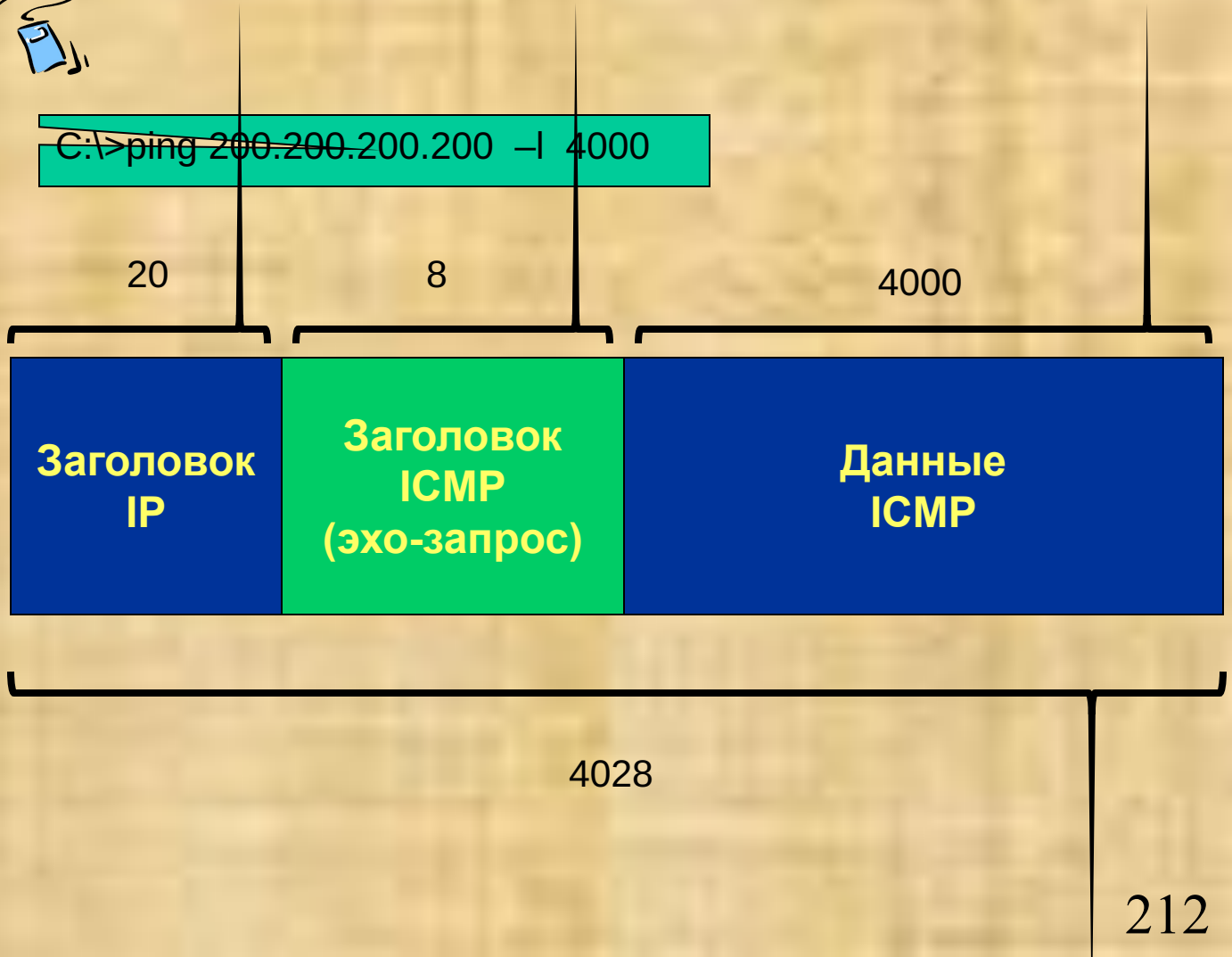
1. Адрес данного узла
2. Адреса, рекомендуемые для внутренних сетей
3. Адреса для группового вещания (224.0.0.0 – 239.255.255.255)
4. Адреса класса E (240.0.0.0 – 247.255.255.255)
5. Адреса типа «обратная петля» 127.x.x.x
6. Некорректные адреса (например, 0.0.0.0)

Фрагментация

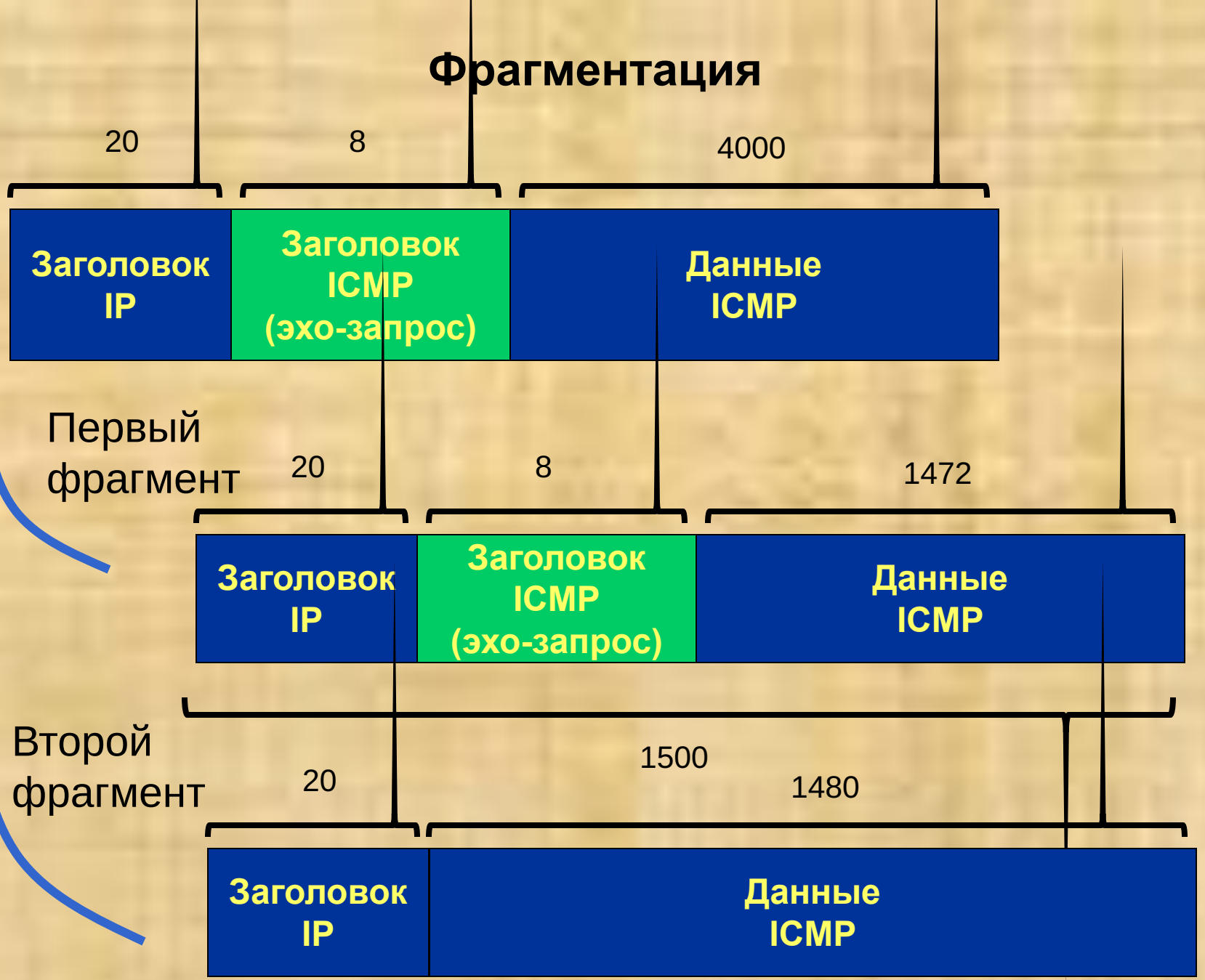


Фрагментация



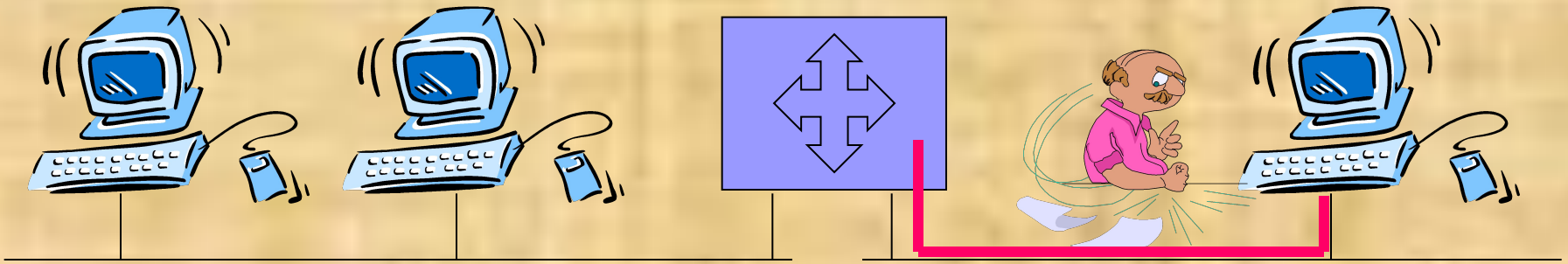


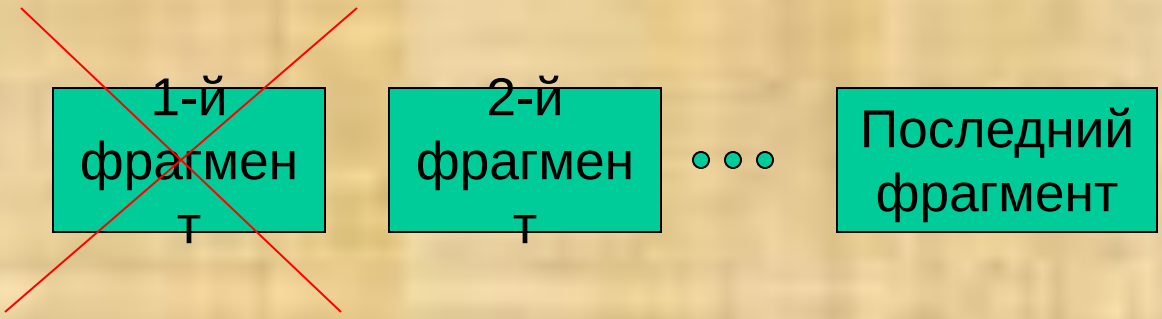
Фрагментация



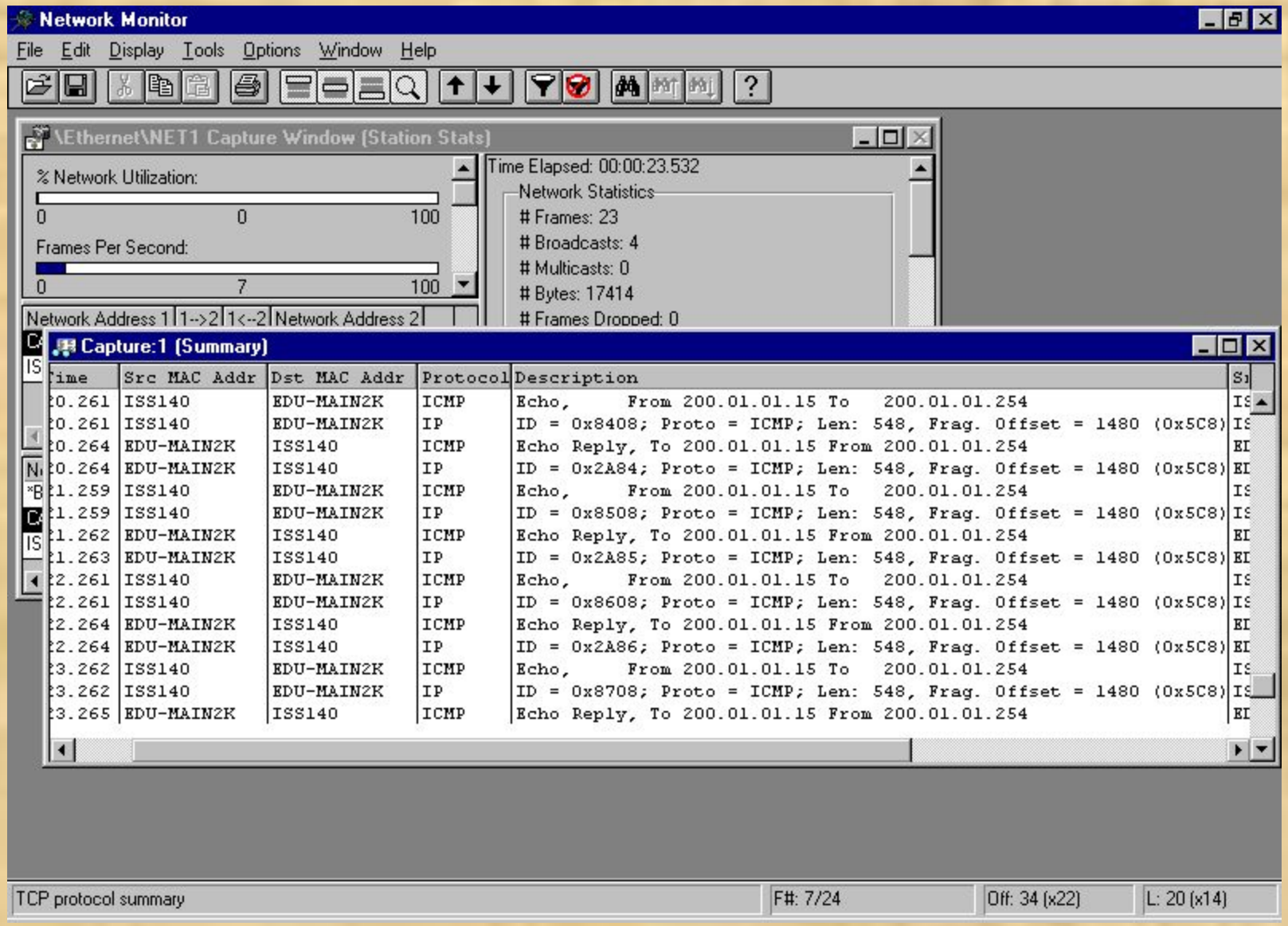
Фрагментация

Фрагментация с целью обхода фильтрации





Фрагментация с целью обхода фильтрации



Ошибки реализации функции фрагментации

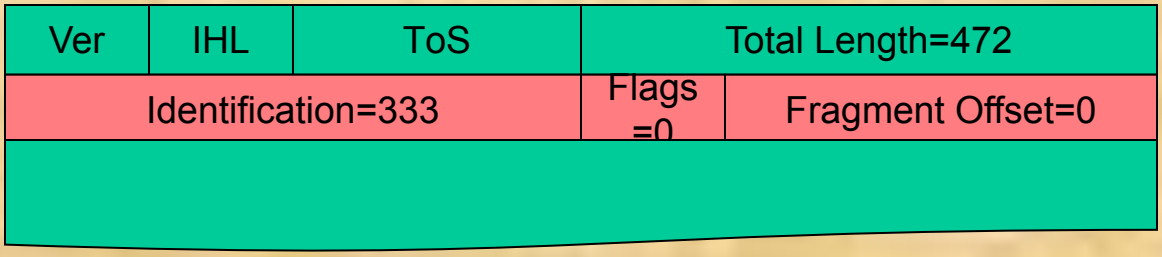
Атака Teardrop

Атака IP DoS Fragmenting (jolt2)

Атака Ping of Death

Фрагментация

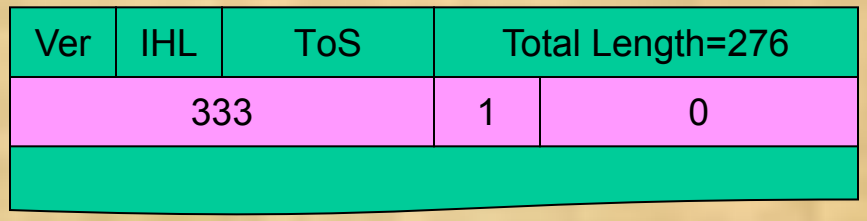
Заголовок исходной датаграммы (до фрагментации)



Заголовок=20 байт

Данные=452 байта

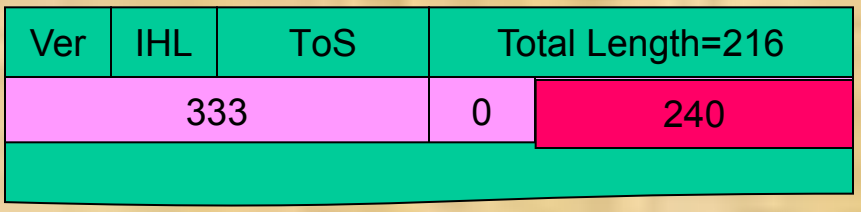
Заголовок 1-го фрагмента



Flags= 0 0 1

Данные=256 байт

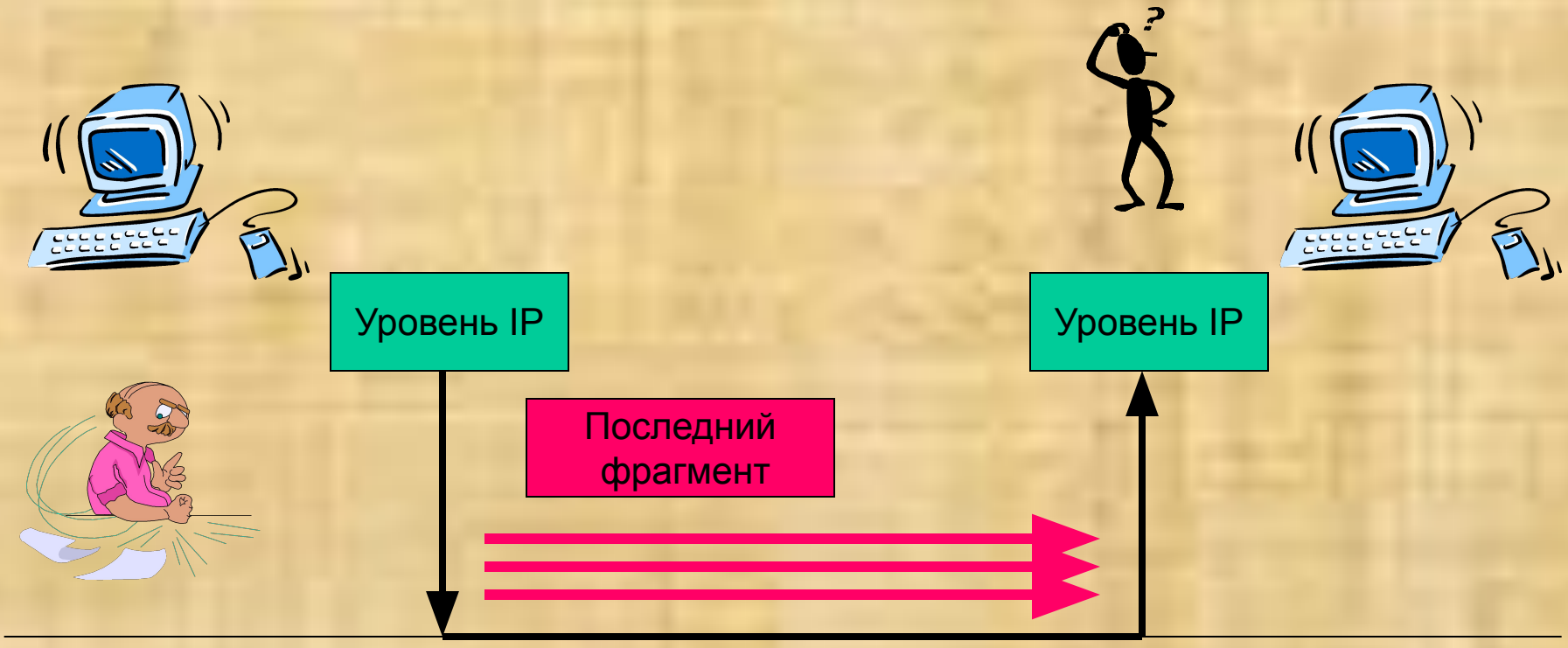
Заголовок 2-го фрагмента



Данные=196 байт

есть следующий фрагмент

Ошибки реализации функции фрагментации

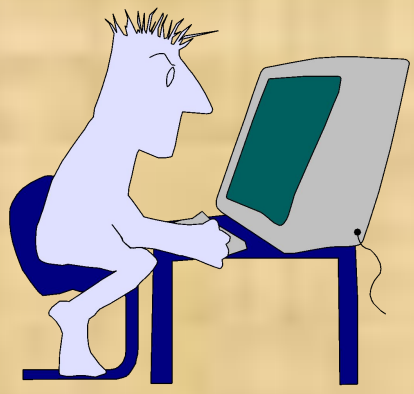


Атака IP DoS Fragmenting (jolt2)

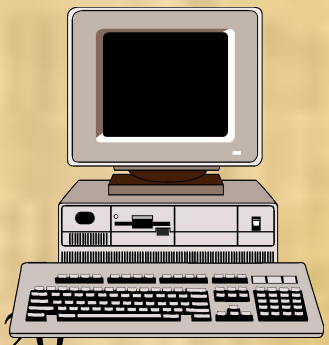
Атака Ping of Death

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

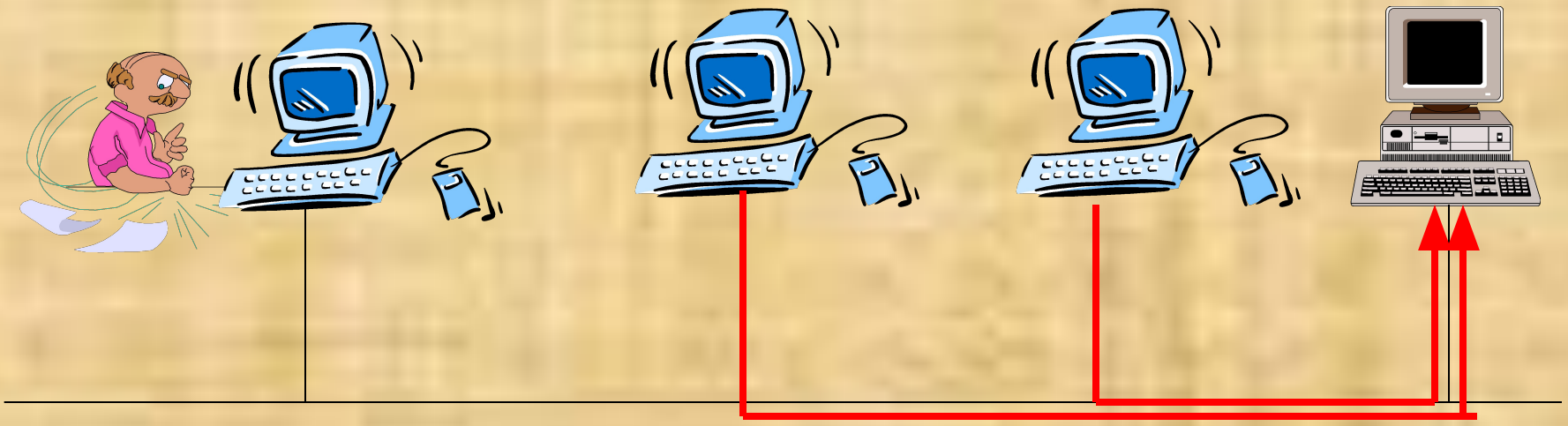
ICMP Timestamp

Smurf

Атака Smurf

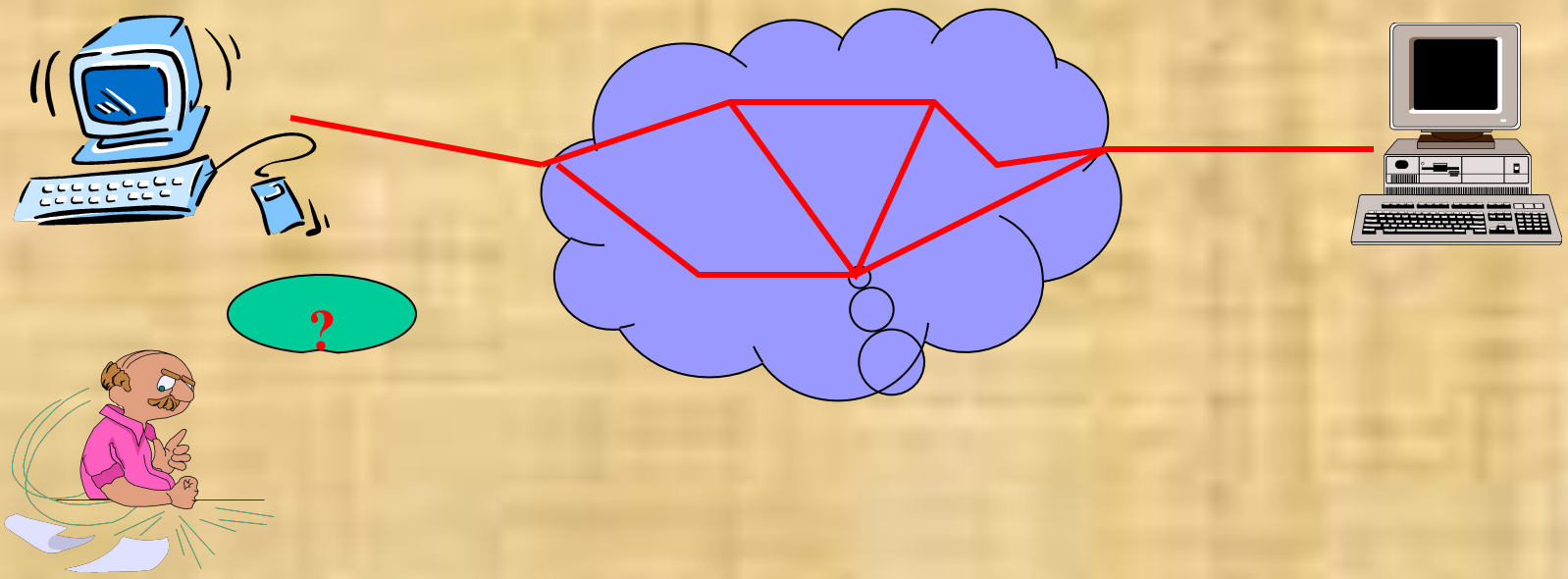
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol=ICMP	Header Checksum	
Адрес объекта атаки			
Адрес сети или широковещательный			
Options			Padding

Атака Smurf



ICMP-ответы от всех узлов сегмента

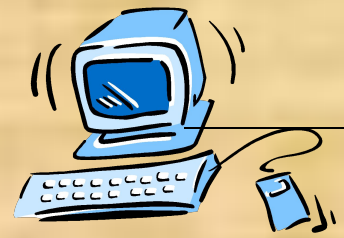
Отслеживание маршрутов



- Протокол ICMP
- Протокол UDP

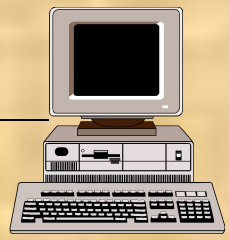
Отслеживание маршрутов - пример

Windows – утилита **tracert**

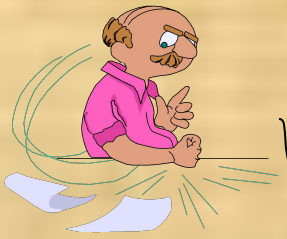


200.0.0.135

200.2.2.254



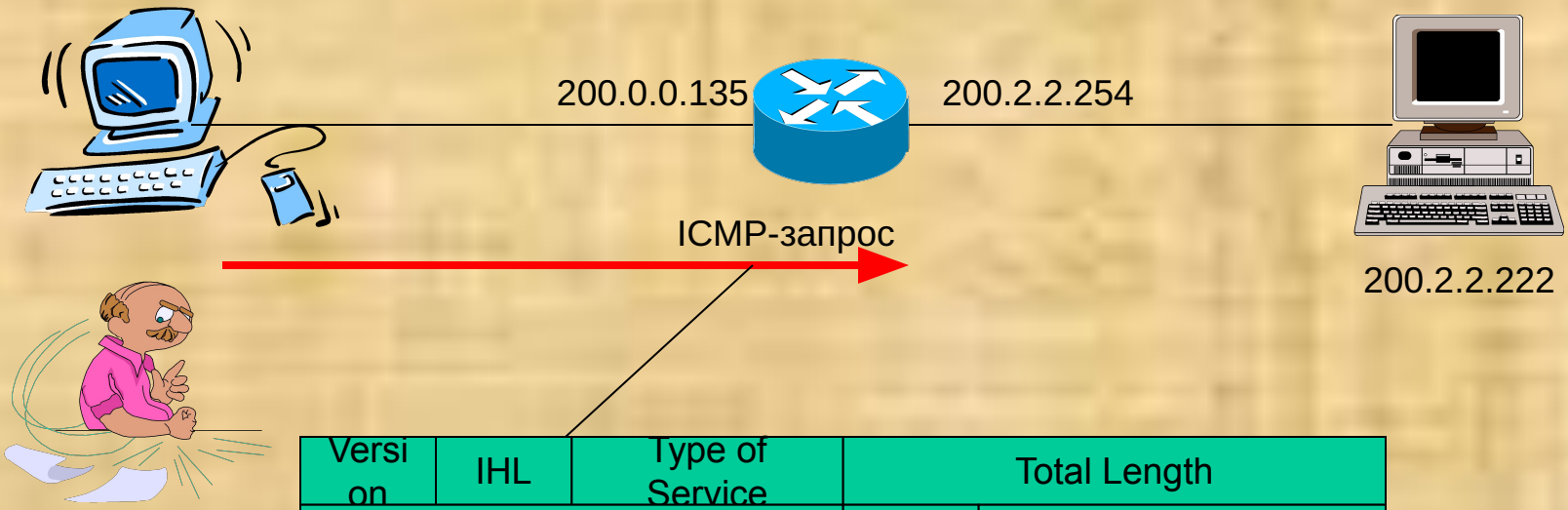
200.2.2.222



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

Отслеживание маршрутов - пример

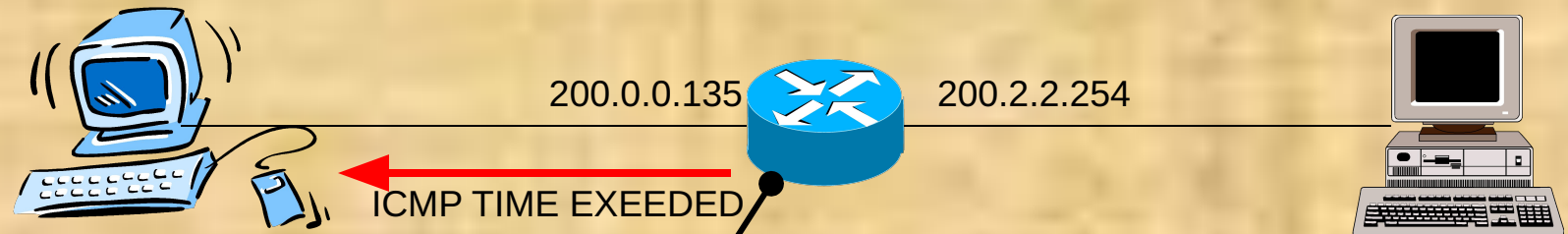
Windows – утилита **tracert**

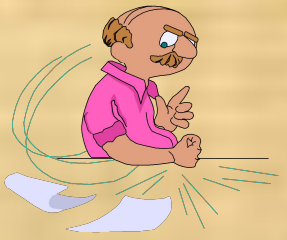


Versi on	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL=1		**Protocol=ICM P**	Header Checksum	
200.0.0.x				
200.2.2.222				
Options				Padding

Отслеживание маршрутов - пример

Windows – утилита **tracert**

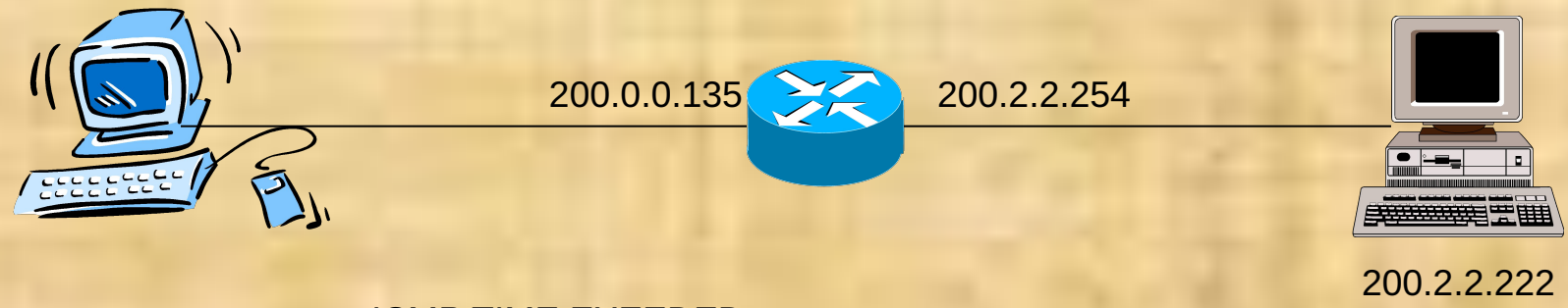




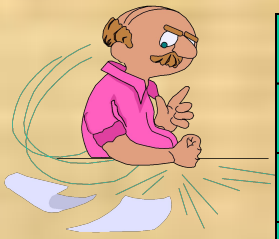
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL= 0		Protocol=ICMP	Header Checksum	
200.0.0.x				
200.2.2.222				
Options				Padding

Отслеживание маршрутов - пример

Windows – утилита **tracert**

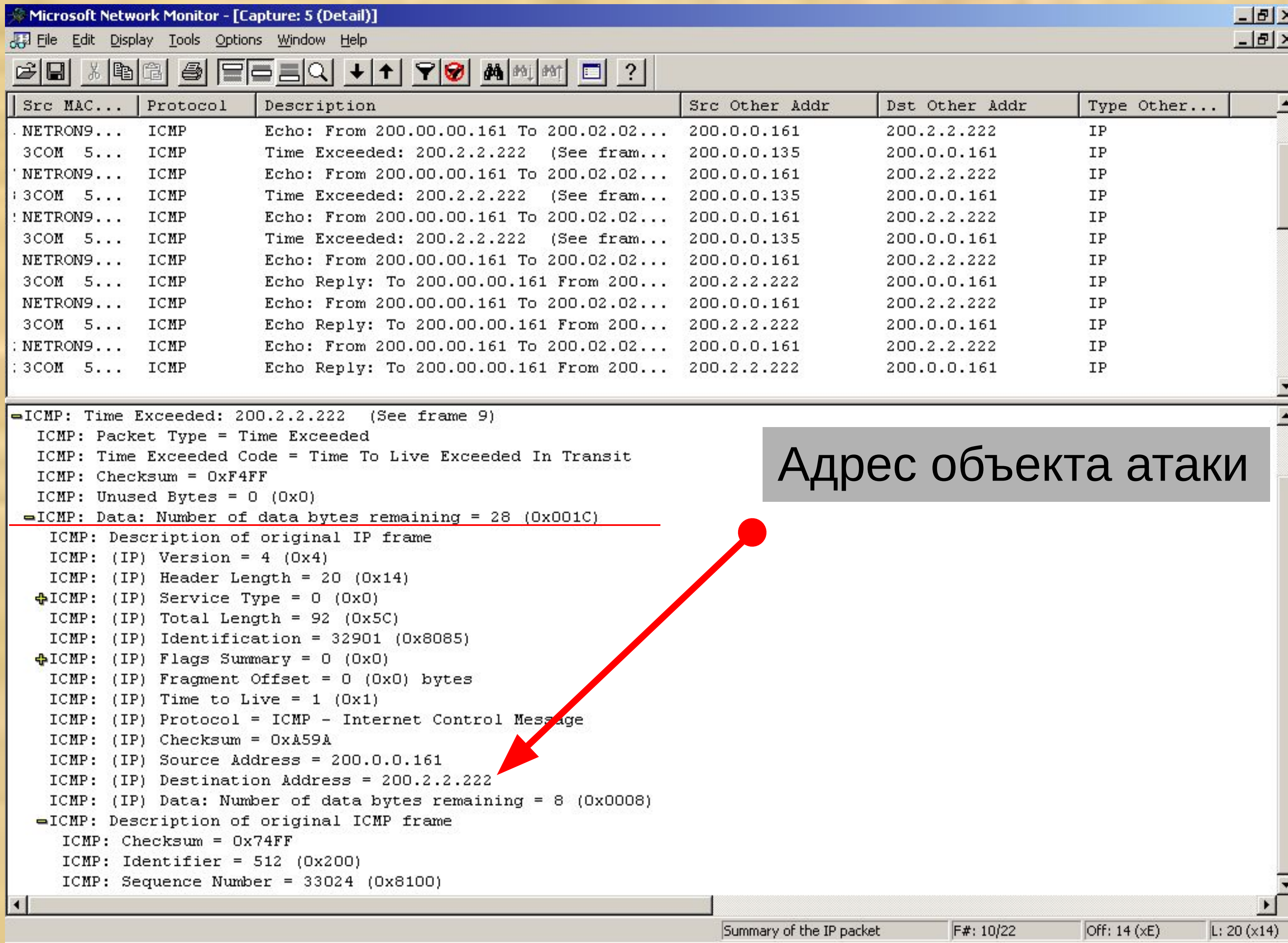


ICMP TIME EXEEDED

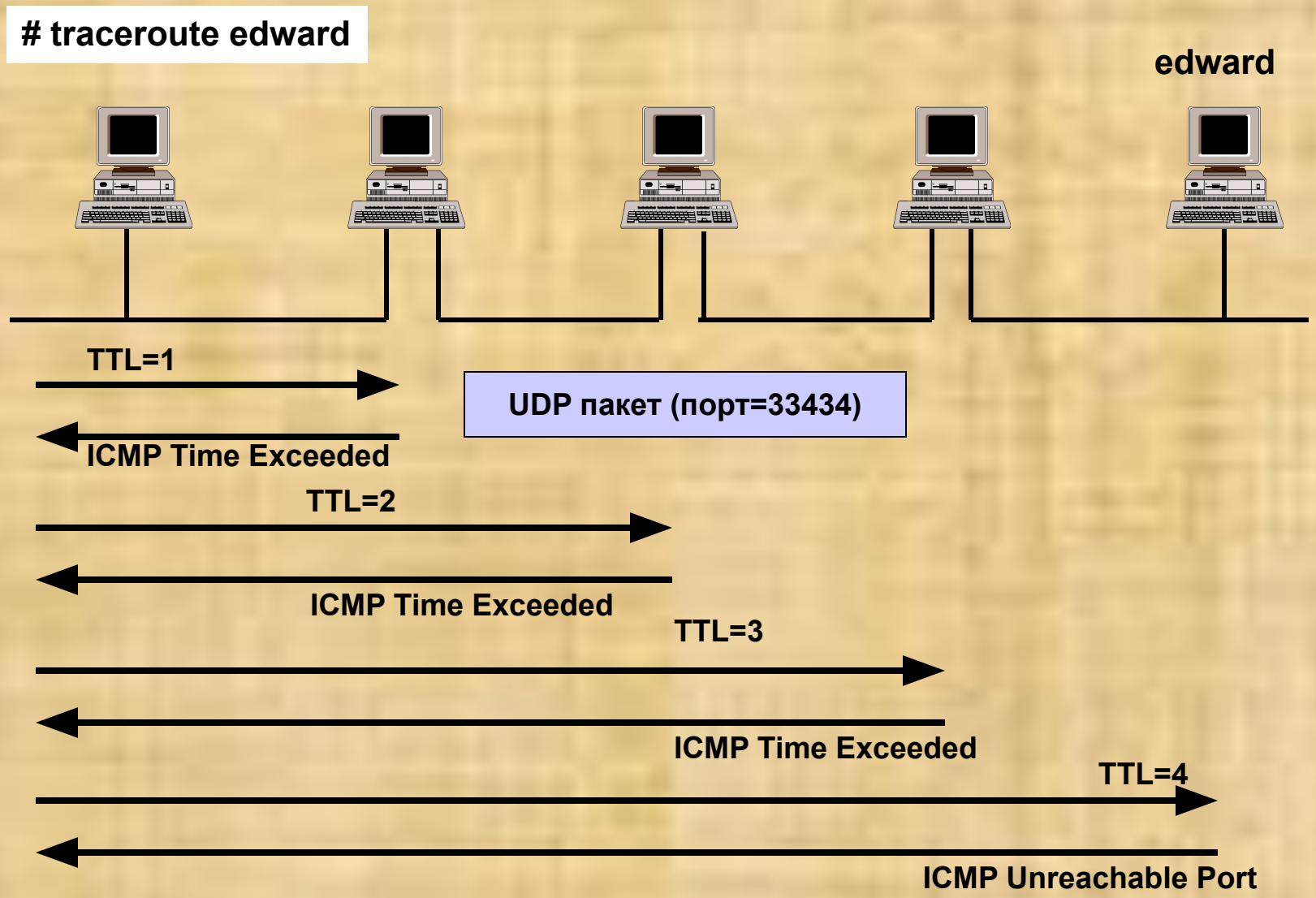


Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol=ICMP	Header Checksum	
200.0.0.135			
200.0.0.x			
Options			Padding
ICMP Data Отправитель – 200.0.0.x **Получатель – 200.2.2.222**			

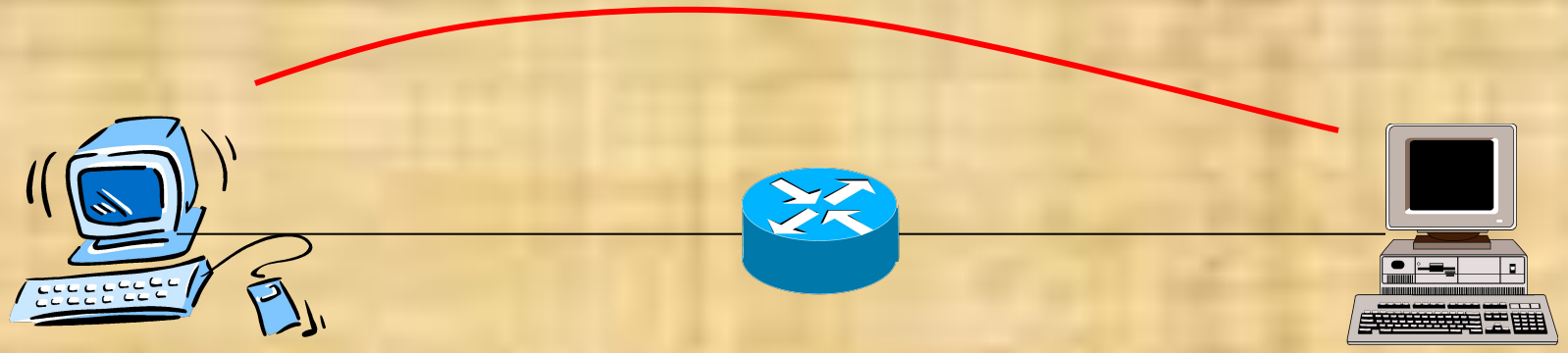
Отслеживание маршрутов - пример



Отслеживание маршрутов (UDP+ICMP)



Практическая работа 4



Определить с помощью сетевого анализатора адрес объекта атаки по сообщению ICMP_TIME_EXEEDED