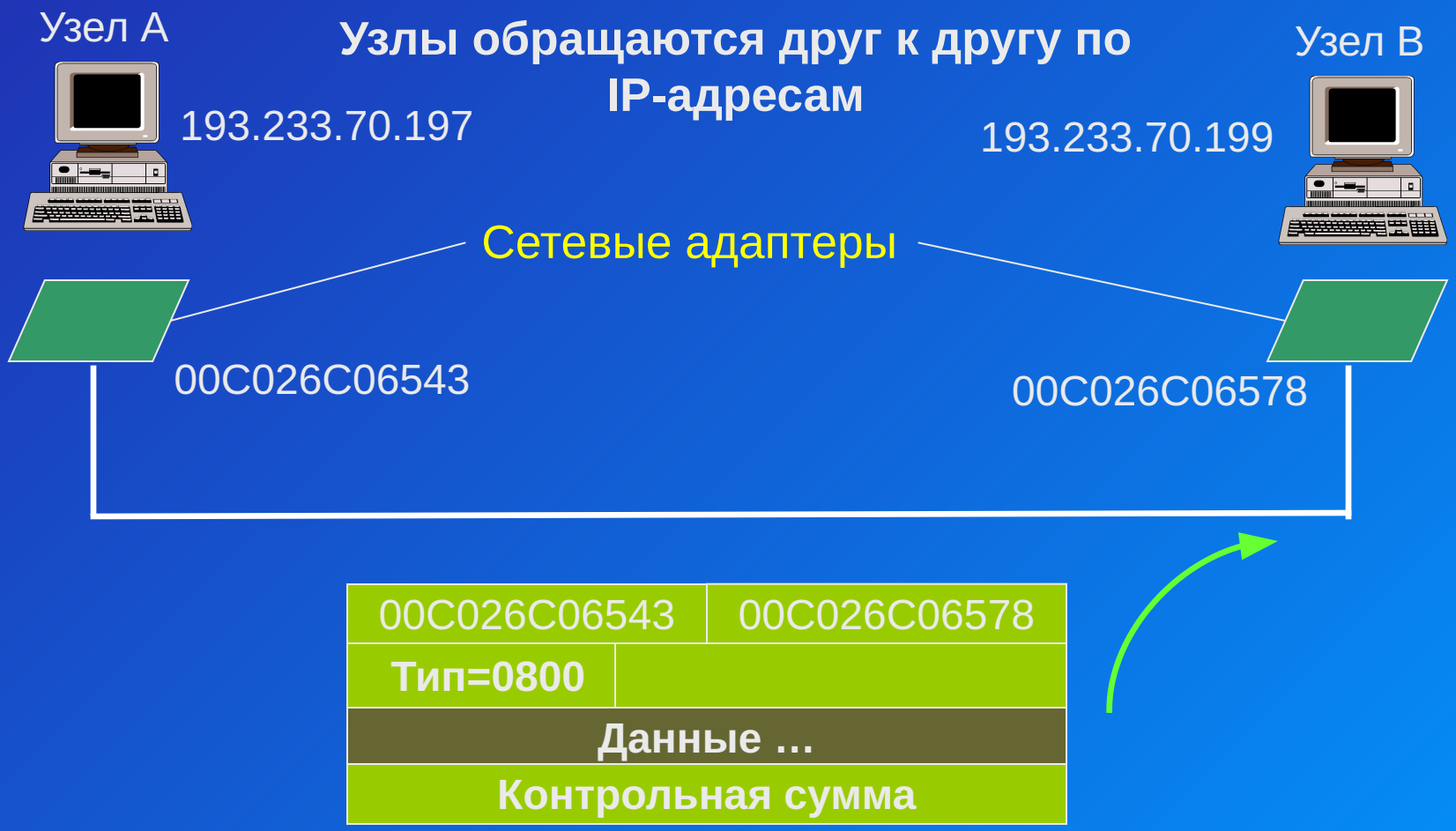
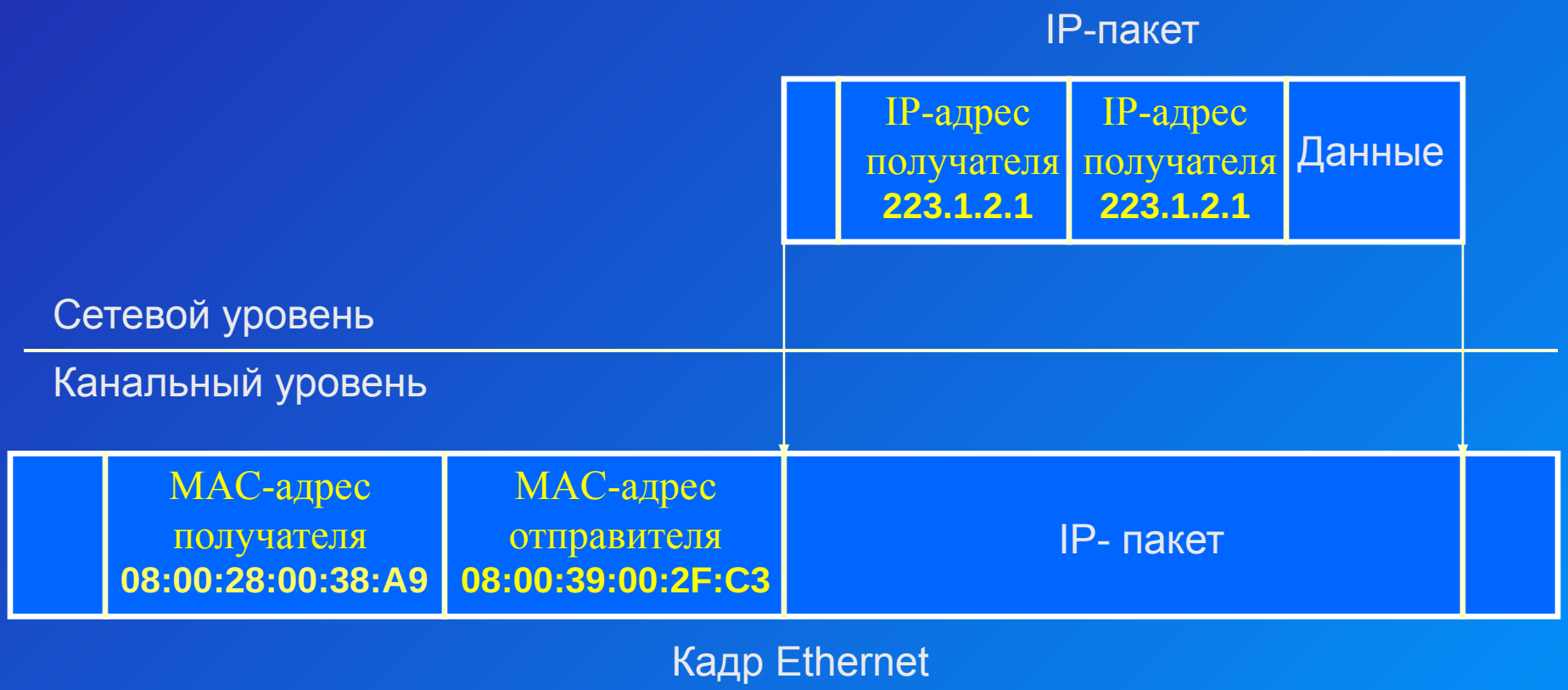
Протокол ARP

Назначение протокола ARP



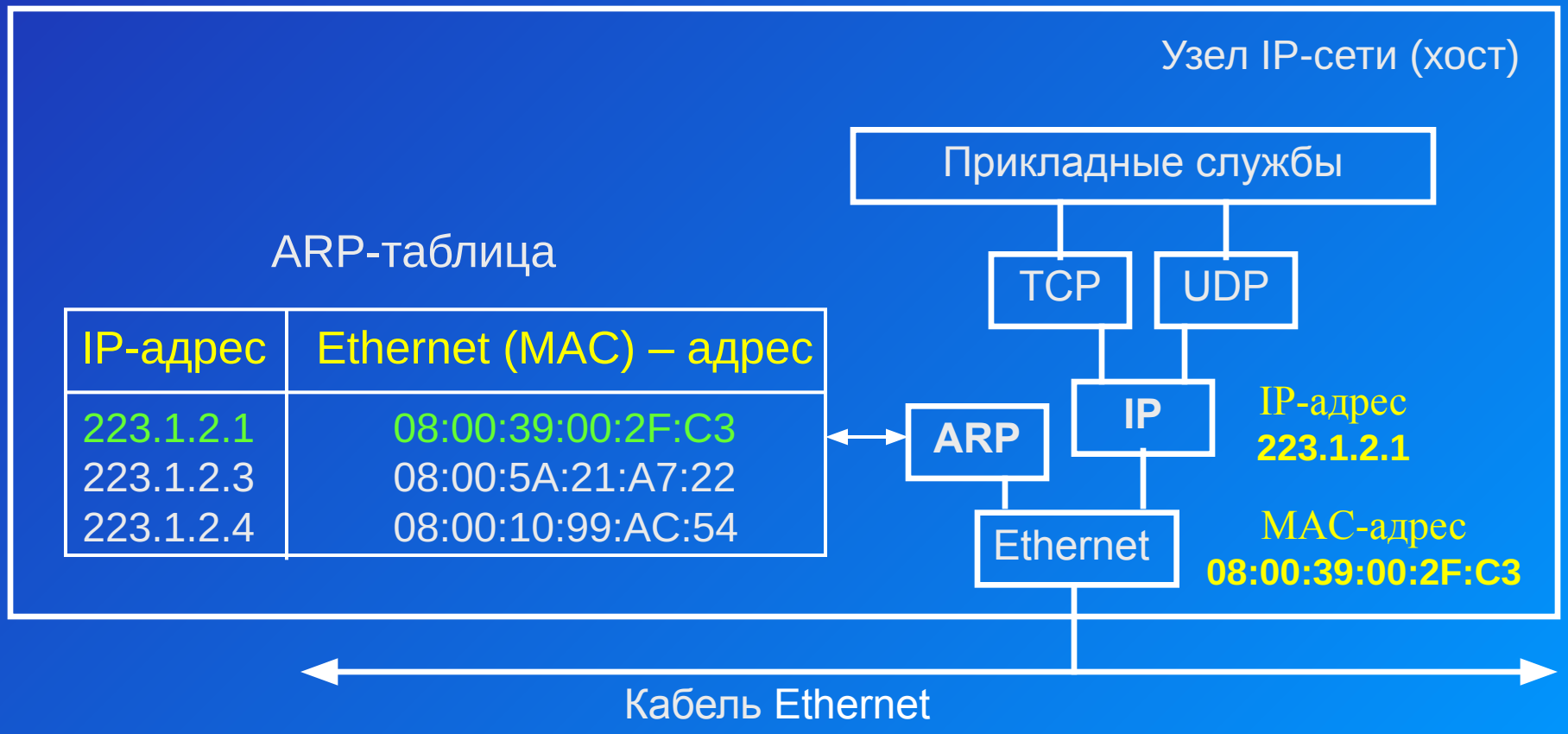
По сети передаются пакеты, содержащие адреса сетевых адаптеров

Инкапсуляция IP-пакетов в кадры Ethernet

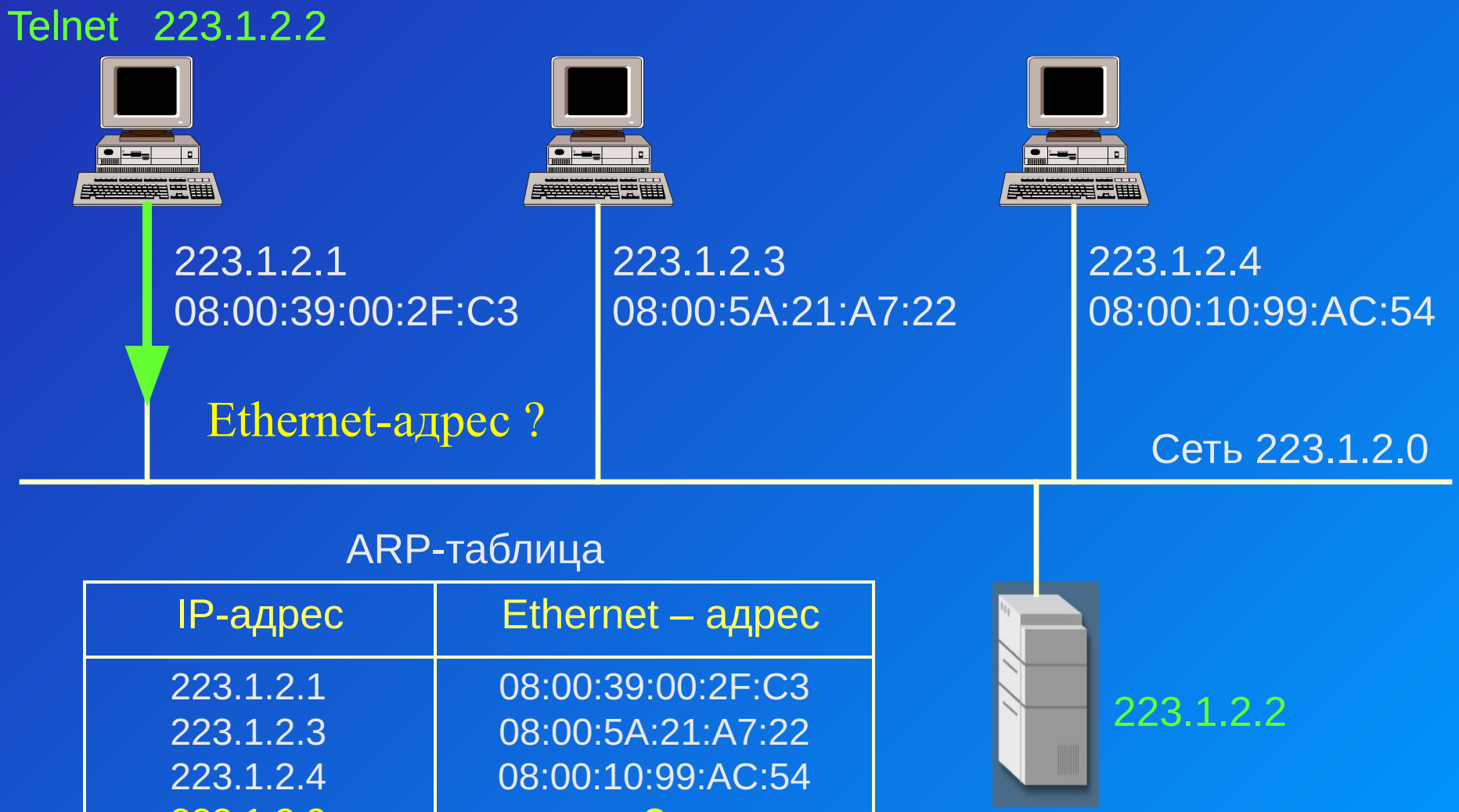


Назначение протокола ARP

Протокол ARP (Address Resolution Protocol - протокол разрешения адресов) используется для определения соответствия IP-адресов и Ethernet-адресов хостов



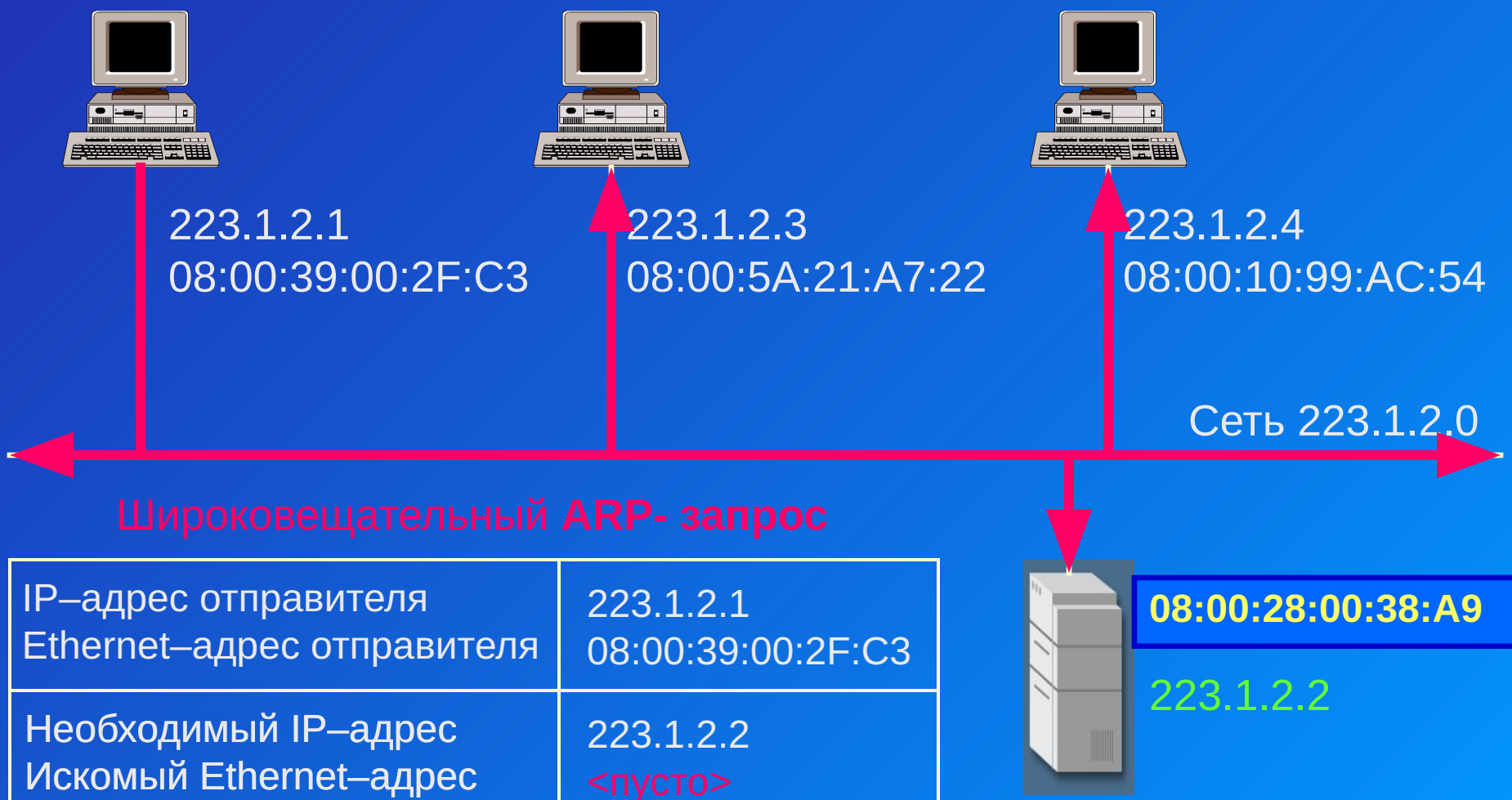
Определение MAC-адреса искомого хоста



ARP-таблица

IP-адрес	Ethernet – адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54
223.1.2.2	?

Определение MAC-адреса искомого хоста



IP–адрес отправителя Ethernet–адрес отправителя	223.1.2.1 08:00:39:00:2F:C3
Необходимый IP–адрес Искомый Ethernet–адрес	223.1.2.2 <пусто>

Определение MAC-адреса искомого хоста

223.1.2.1
08:00:39:00:2F:C3

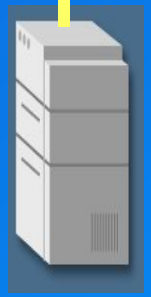
223.1.2.3
08:00:5A:21:A7:22

223.1.2.4
08:00:10:99:AC:54

Сеть 223.1.2.0

ARP- ответ

IP–адрес отправителя Ethernet–адрес отправителя	**223.1.2.2** 08:00:28:00:38:A9
Необходимый IP–адрес Искомый Ethernet–адрес	**223.1.2.1** 08:00:39:00:2F:C3



08:00:28:00:38:A9

223.1.2.2

Определение MAC-адреса искомого хоста

Telnet 223.1.2.2

223.1.2.1
08:00:39:00:2F:C3

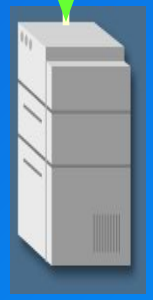
223.1.2.3
08:00:5A:21:A7:22

223.1.2.4
08:00:10:99:AC:54

Сеть 223.1.2.0

Модифицированная ARP-таблица

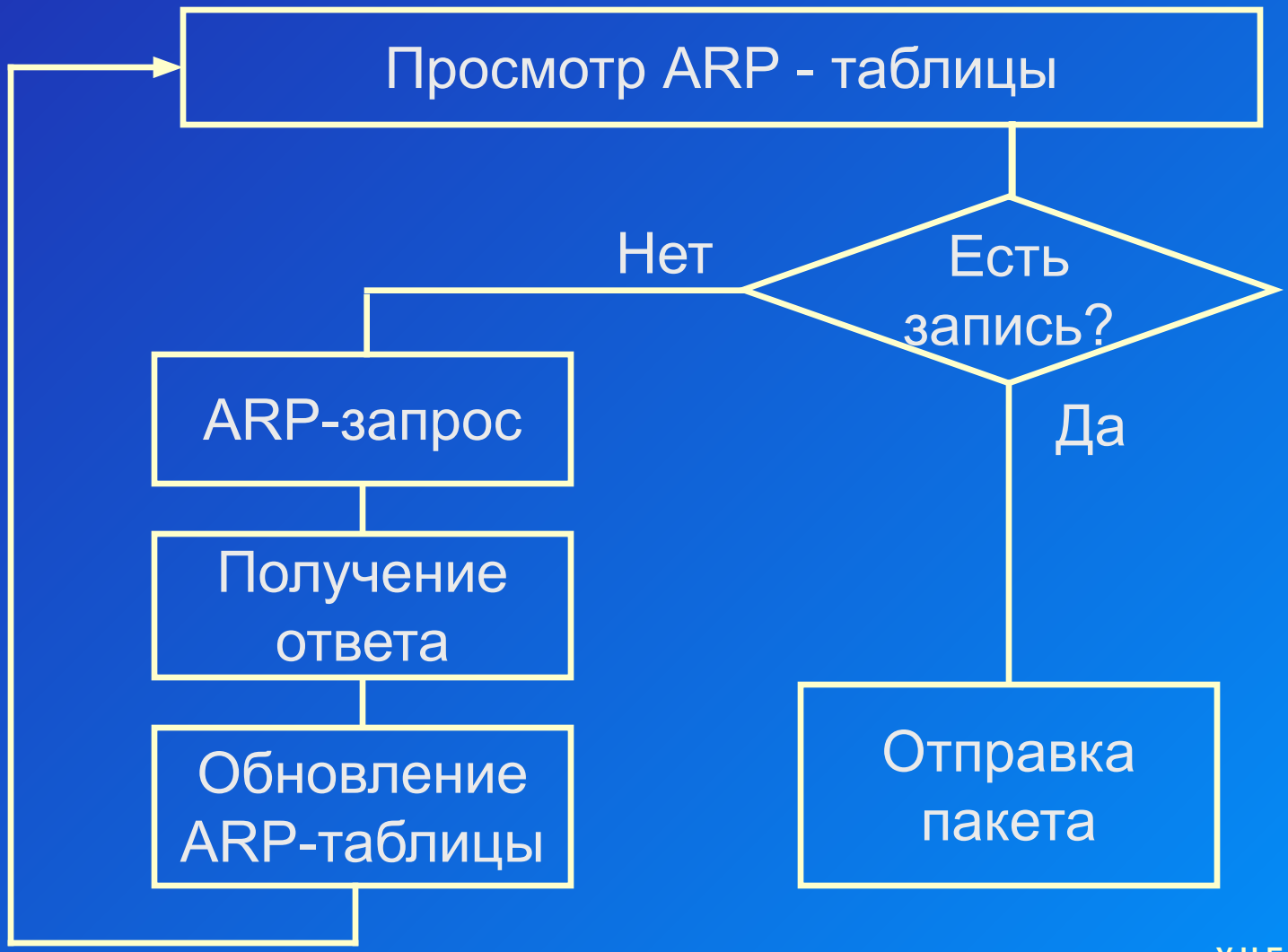
IP-адрес	Ethernet – адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.2	**08:00:28:00:38:A9**
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54



08:00:28:00:38:A9

223.1.2.2

Порядок определения MAC-адреса необходимого хоста

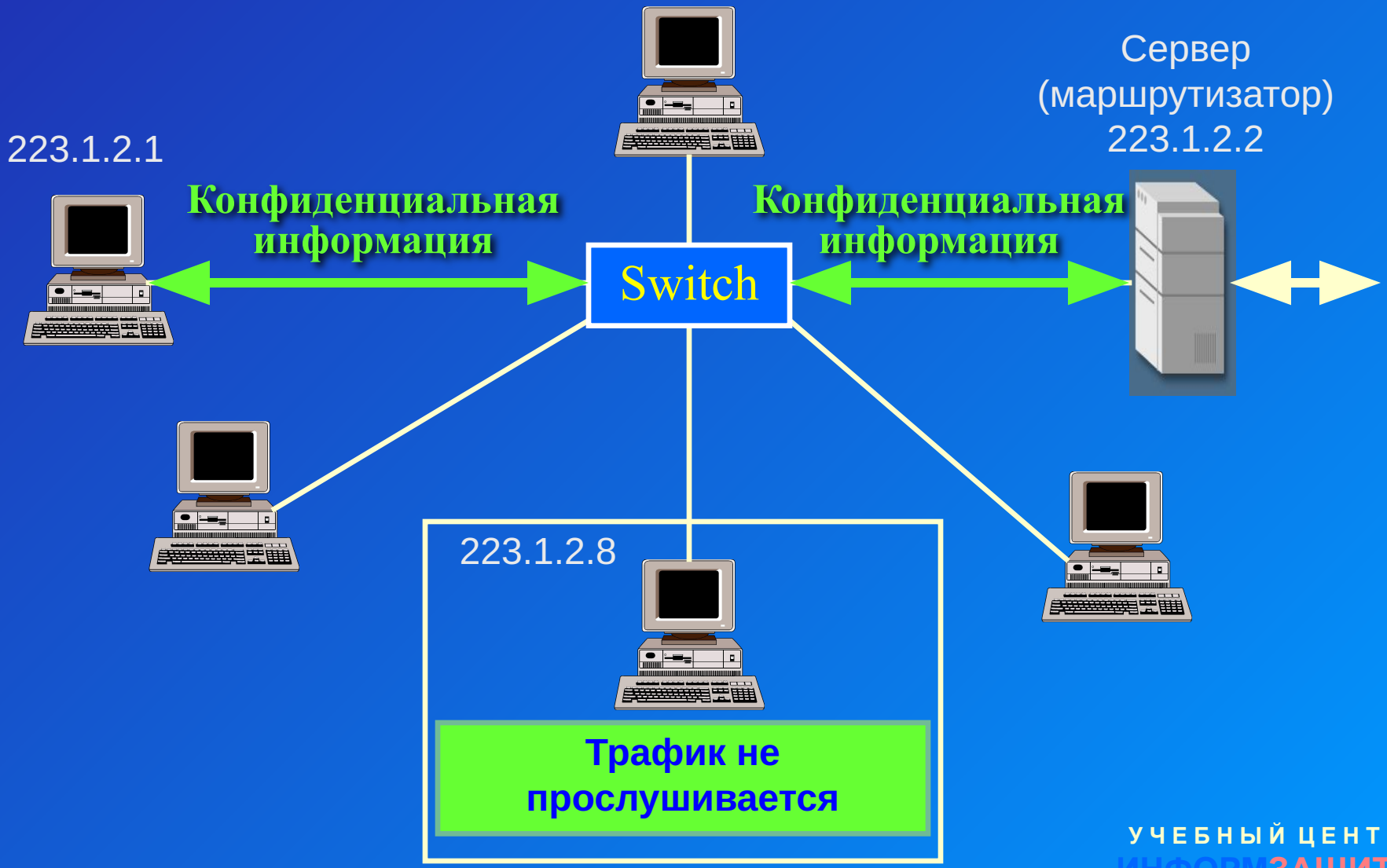


Формат ARP - пакета

Атаки с использованием ARP

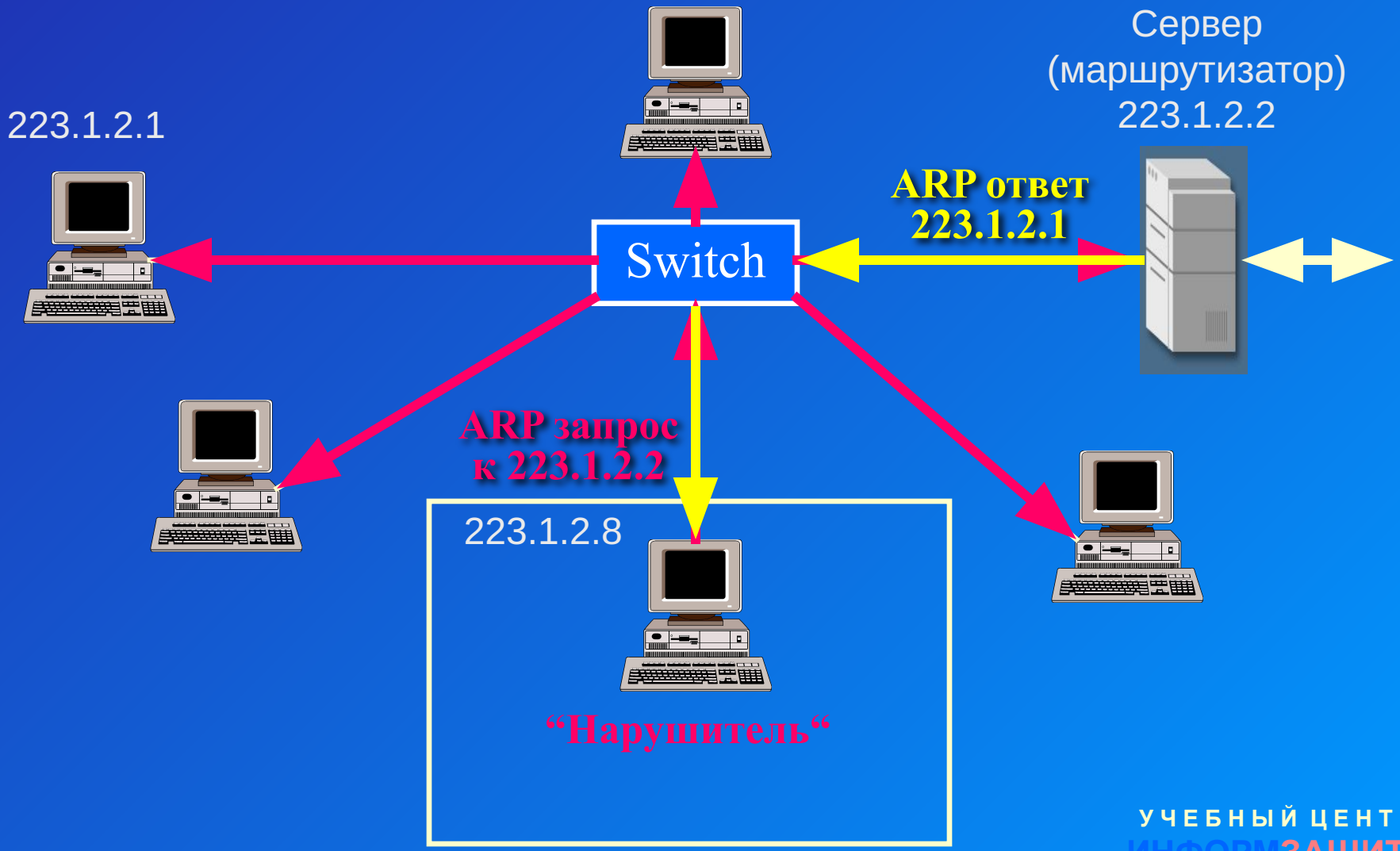
1. ARP-spoofing с целью прослушивания трафика между определенными узлами сегмента IP-сети.
2. Вызов в Windows 95/98/NT сообщений, требующих нажатия кнопки «ОК».

ARP-spoofing или создание ложного IP-посредника



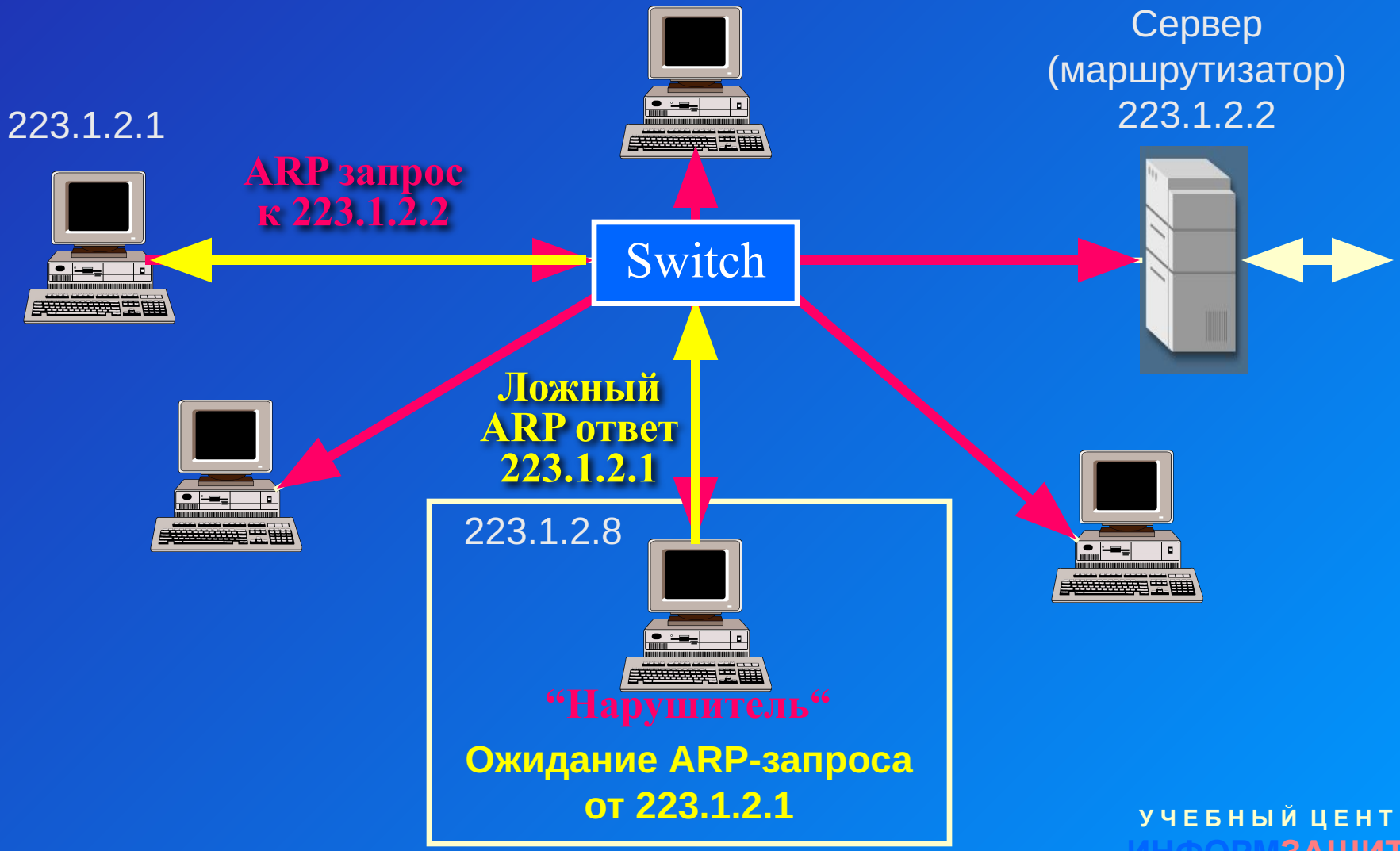
ARP-spoofing или создание ложного IP-посредника

(подготовка к внедрению)



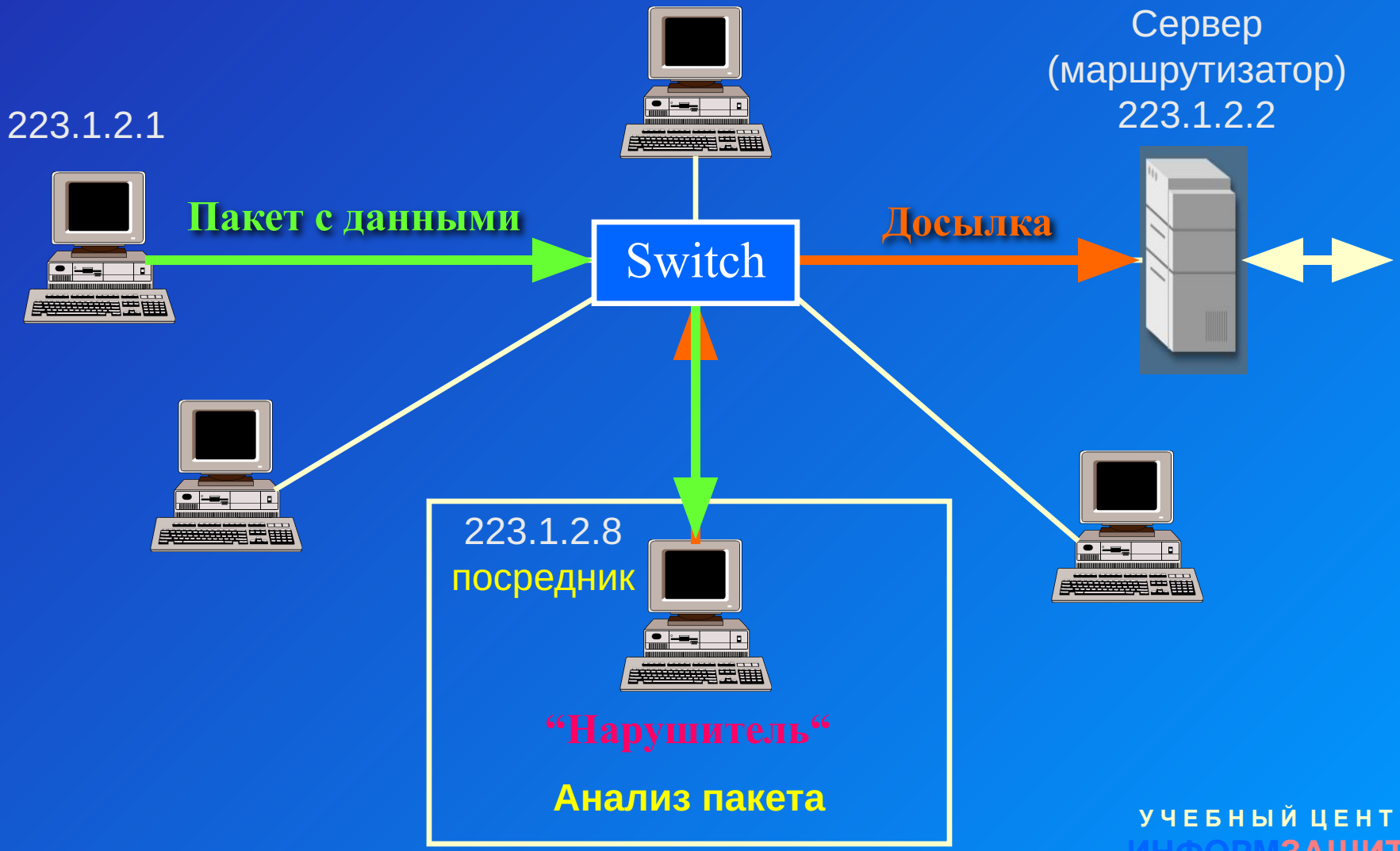
ARP-spoofing или создание ложного IP-посредника

(ожидание ARP-запроса и генерация ложного ARP-ответа)

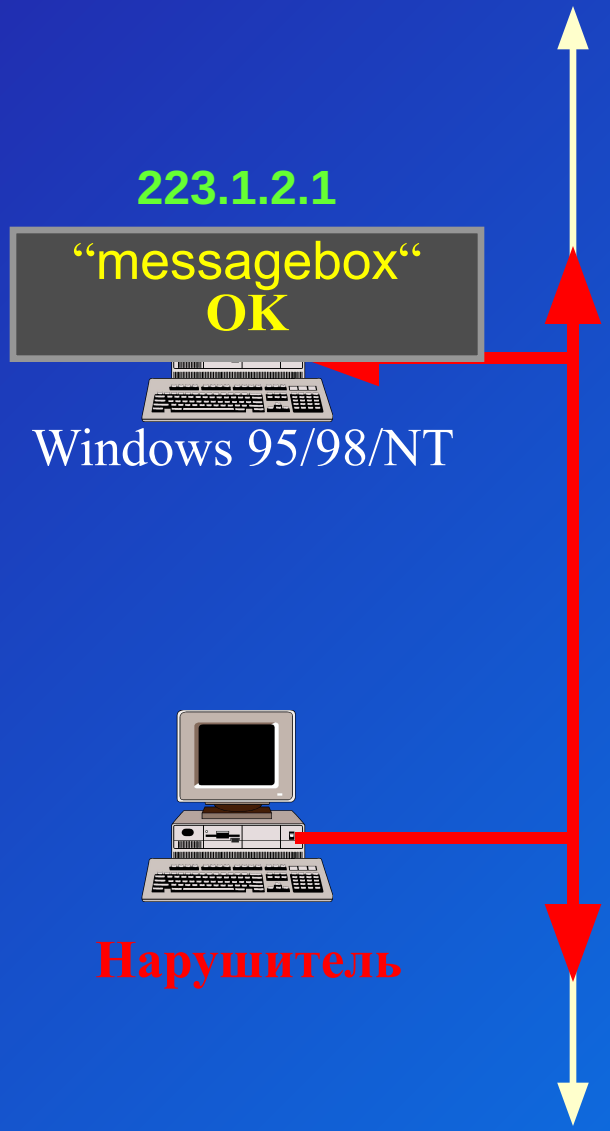


ARP-spoofing или создание ложного IP-посредника

(перехват трафика)



ARP проблемы в Windows 95/98/NT



0	8	16	24	31
Тип сети для Ethernet = 0x0001		Тип протокола для IP = 0x0800		
LHA Eth.= 6	LPA IP = 4	Тип действия для ARP-запроса = 1		
MAC-адрес отправителя (байты 0-3) XXXXXXXX				
(байты 4-5) XXXX		IP отправителя (0-1) **DF 01** (223.1)		
IP отправителя (2-3) **0201** (2.1)		MAC (байты 0-1) XXXX		
MAC-адрес получателя (байты 2-5) XXXXXXXX				
IP-адрес получателя **DF 01 02 01**(233.1.2.1)				