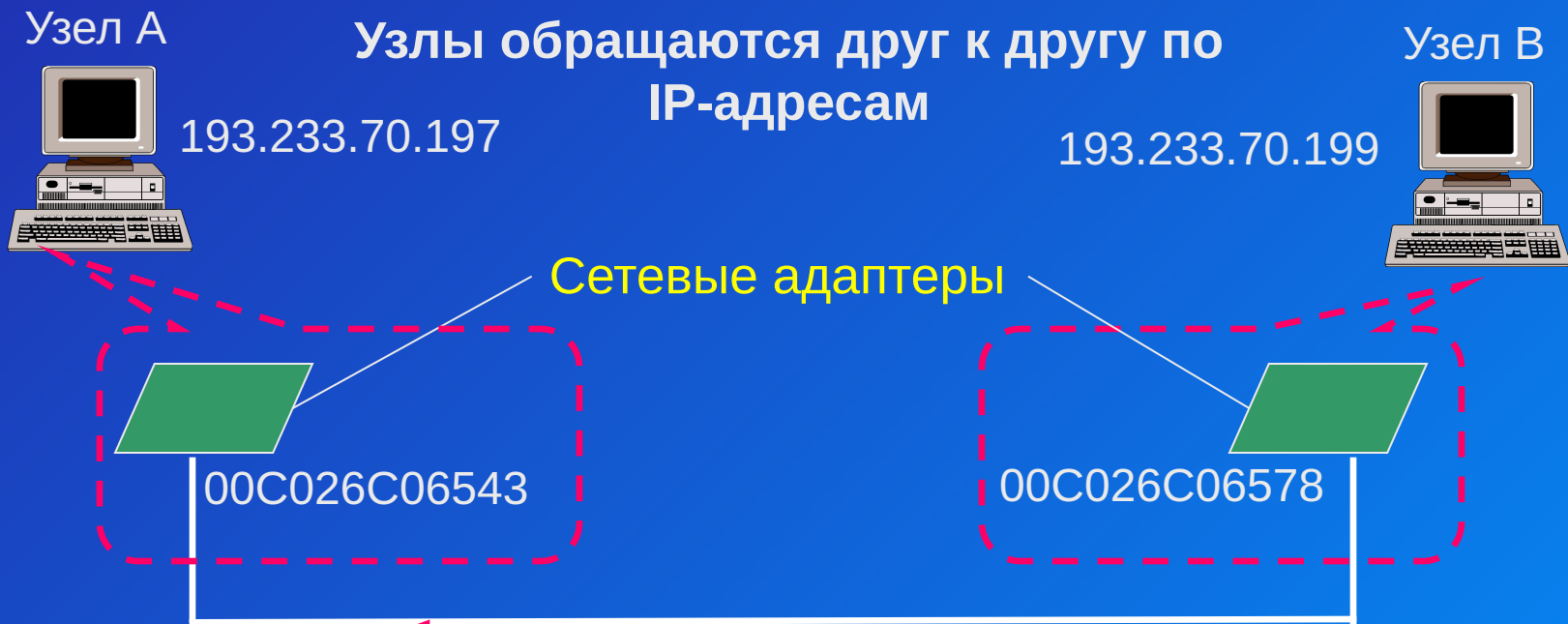


Протокол ARP

Раздел II – Тема 7

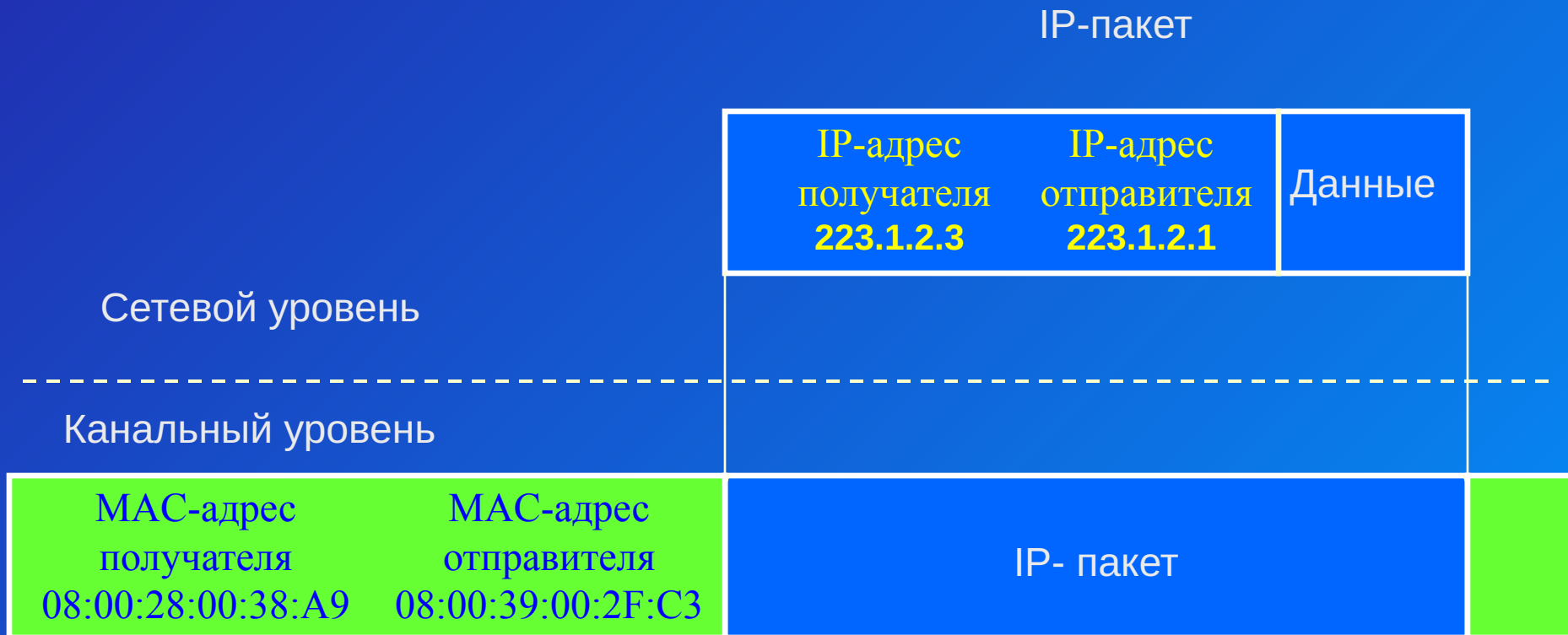
Назначение протокола ARP



Кадр, передаваемый по сети (фрейм)

00C026C06543	00C026C06578
Тип=0800	
Данные ...	
Контрольная сумма	

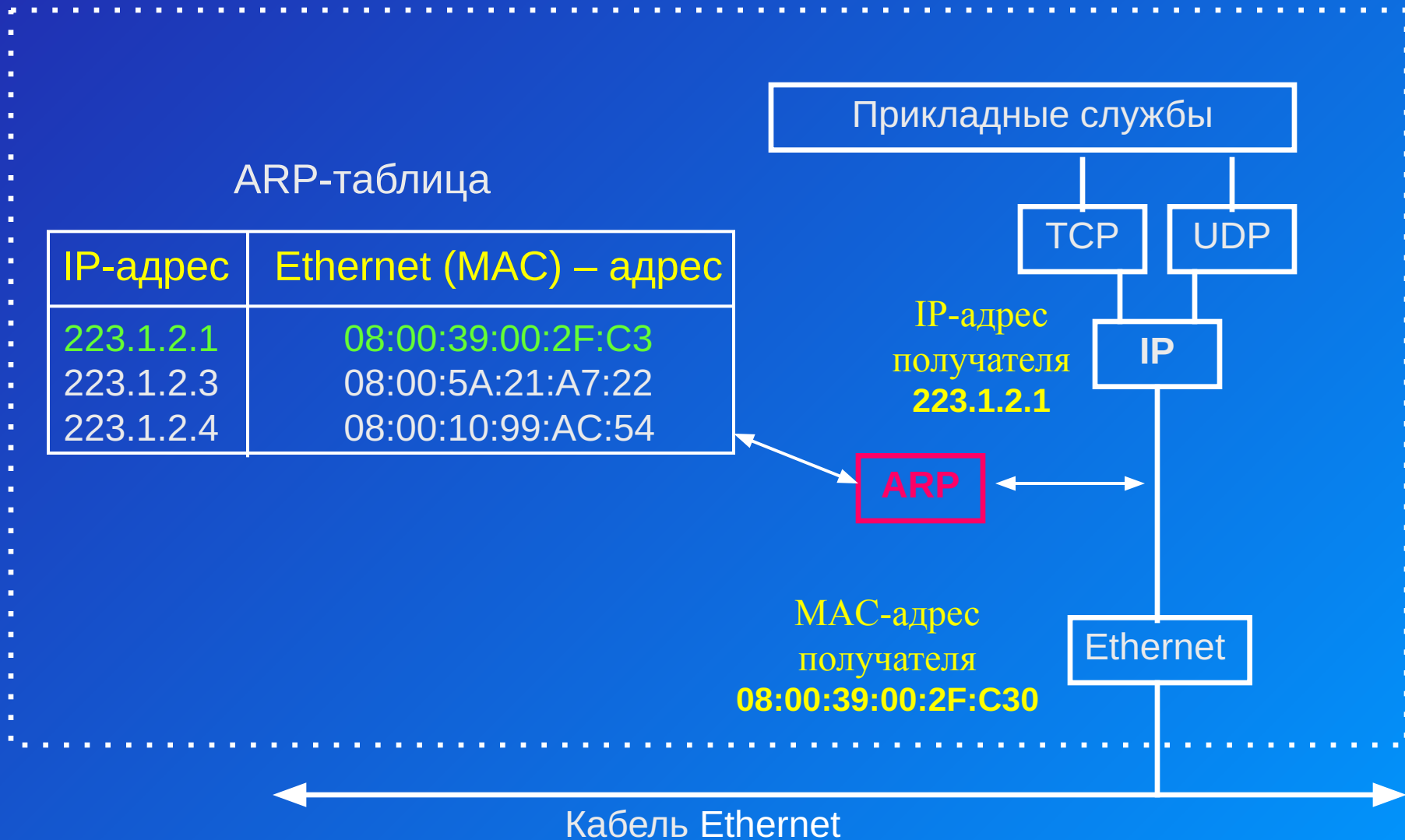
Назначение протокола ARP



Кадр Ethernet



Назначение протокола ARP



Определение MAC-адреса получателя

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

Ethernet-адрес ?

Сеть 223.1.2.0

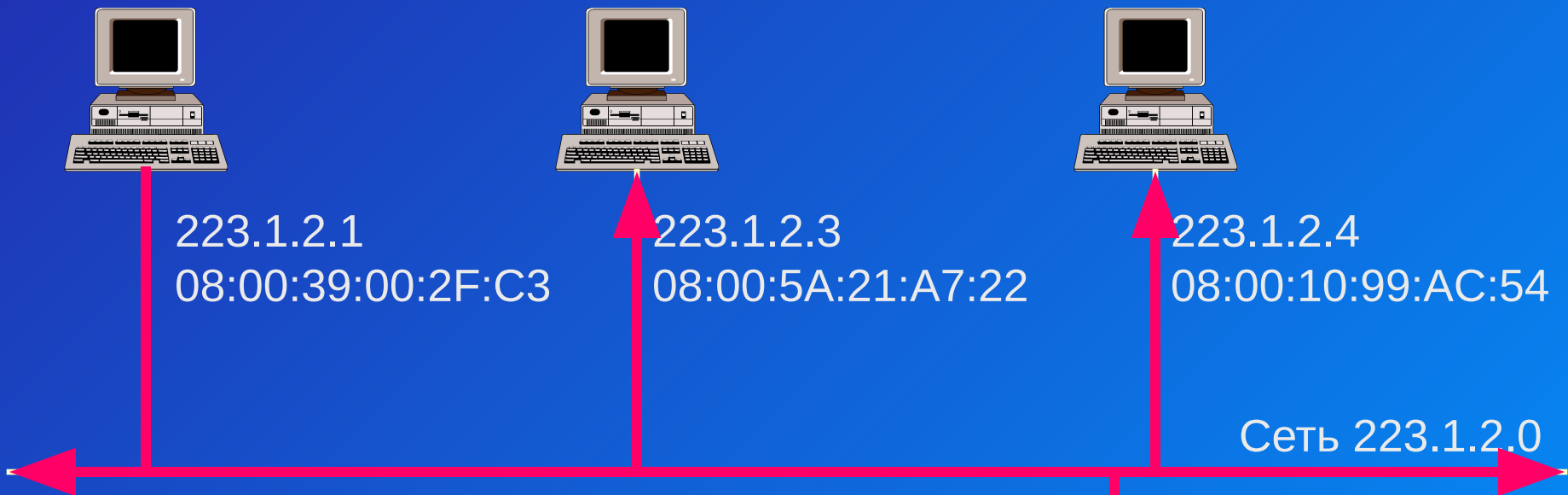
ARP-таблица

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	?



223.1.2.2

Определение MAC-адреса получателя



Широковещательный **ARP-запрос**

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



08:00:28:00:38:A9

223.1.2.2

Определение MAC-адреса получателя



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



08:00:28:00:38:A9

223.1.2.2

Определение MAC-адреса получателя

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

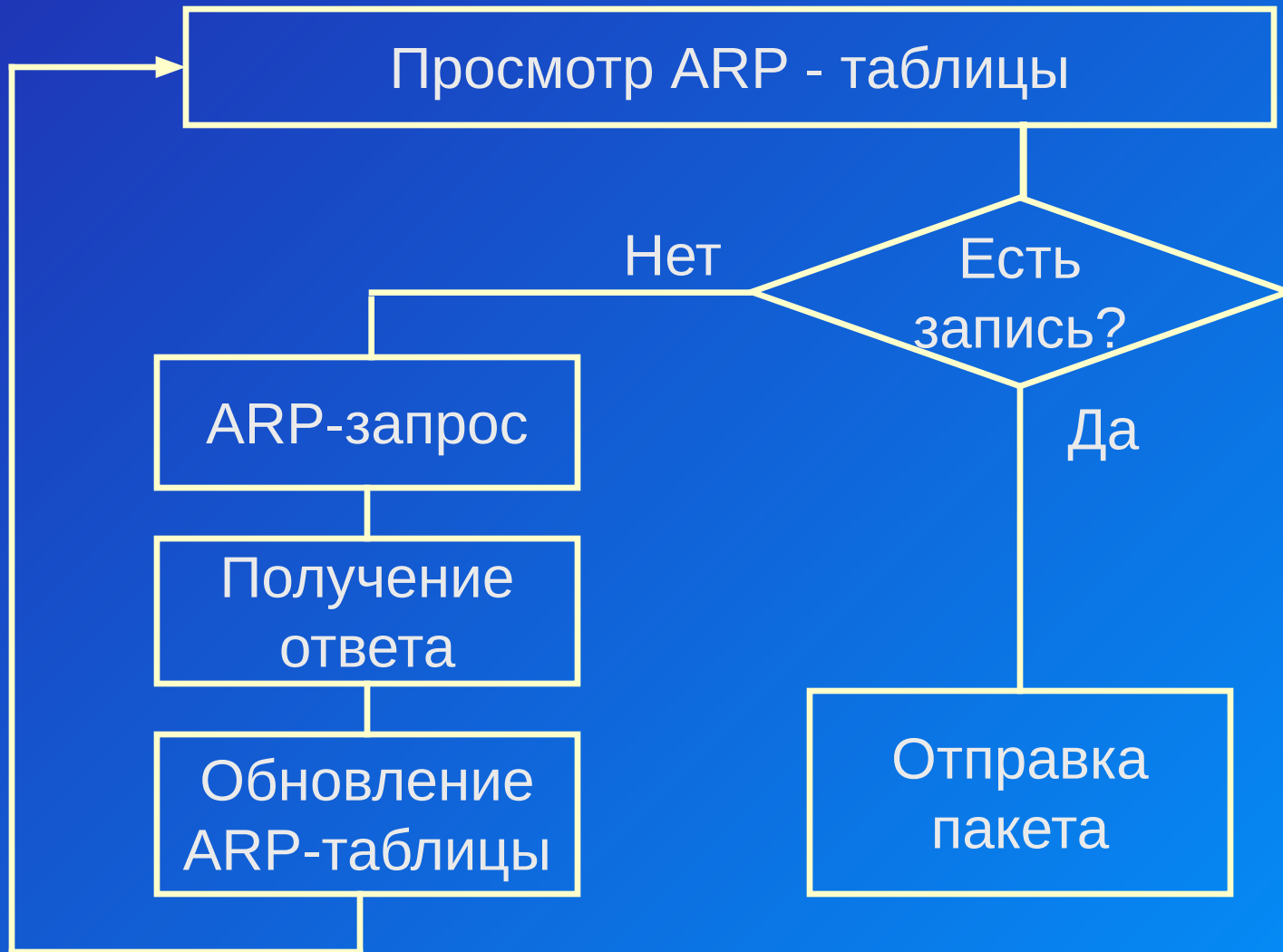
IP-адрес	Ethernet – адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.2	08:00:28:00:38:A9
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54



08:00:28:00:38:A9

223.1.2.2

Схема работы ARP

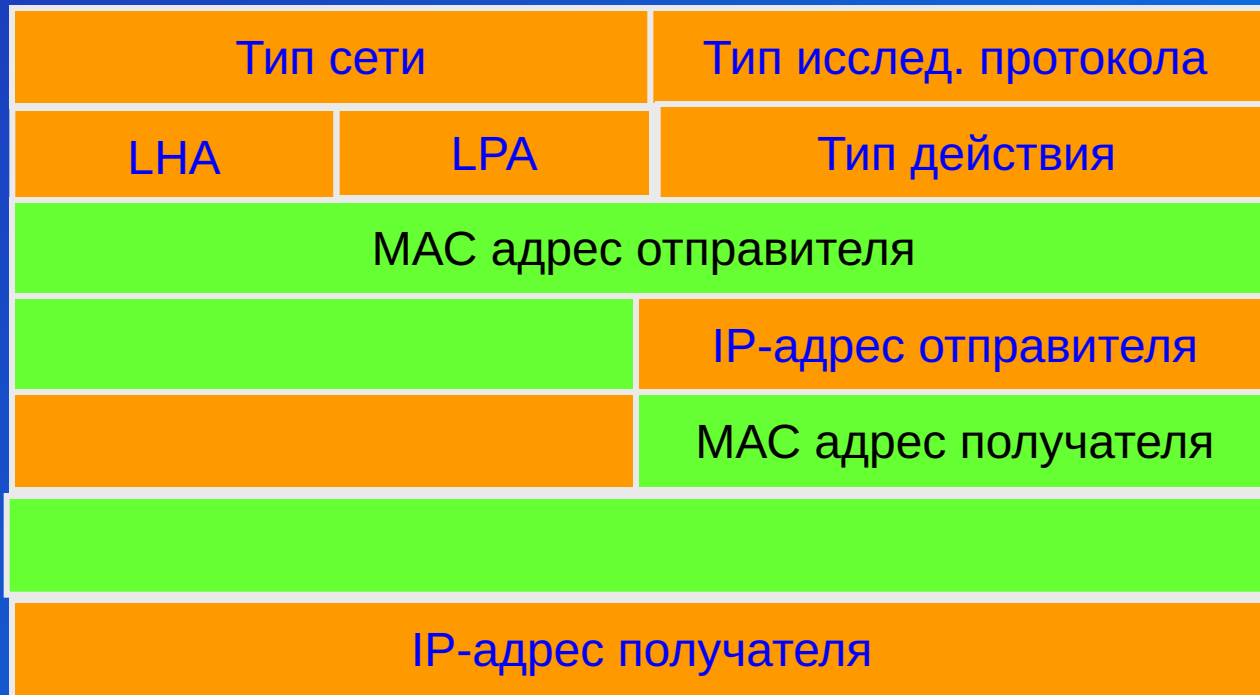


Формат ARP - пакета

0

16

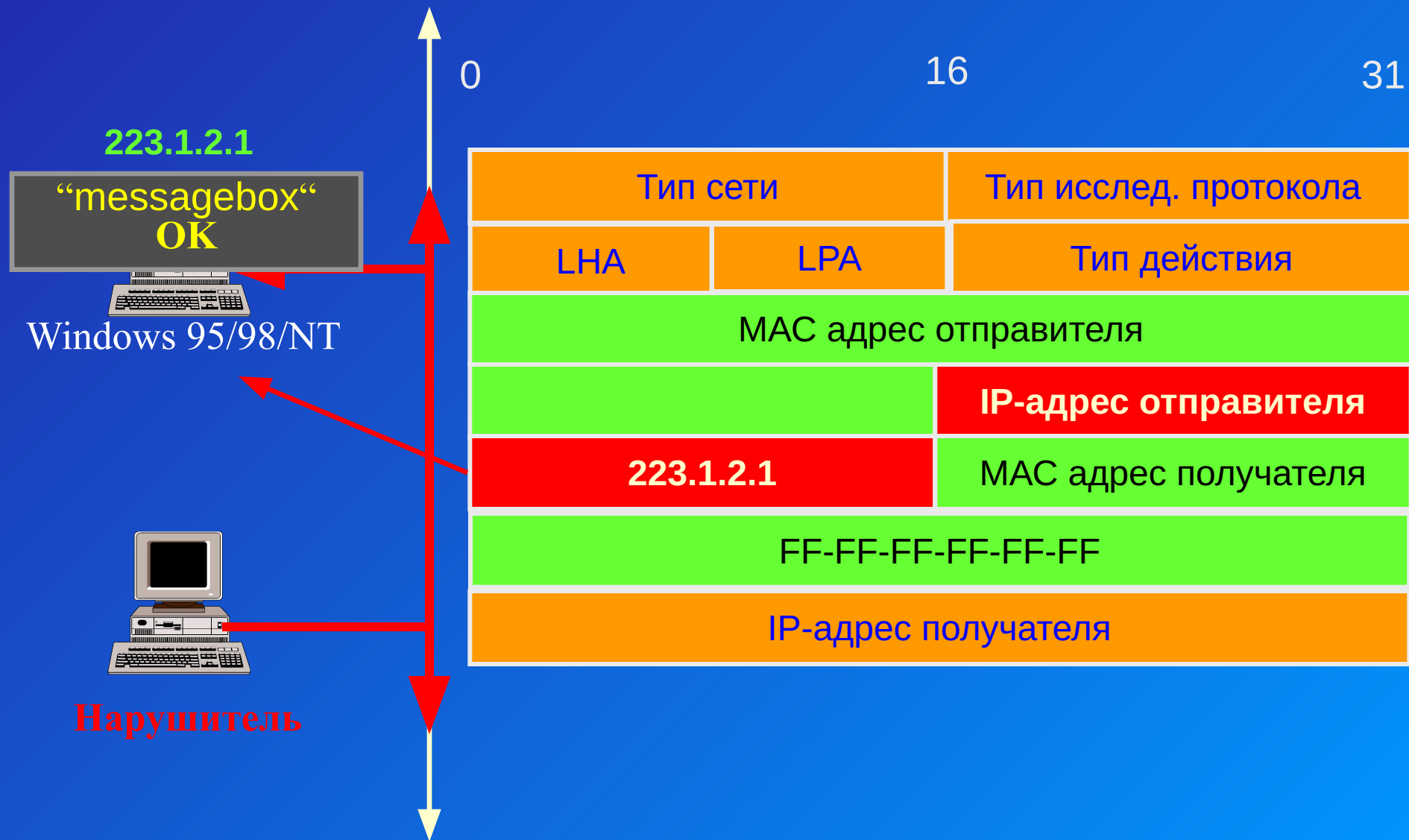
31



Атаки с использованием ARP

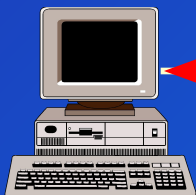
1. Вызов в Windows 95/98/NT сообщений, требующих нажатия кнопки «ОК».
2. ARP-spoofing с целью прослушивания трафика между определенными узлами сегмента IP-сети.

Некорректный ARP -запрос



Некорректный ARP -ответ

223.1.2.1



Объект атаки



0

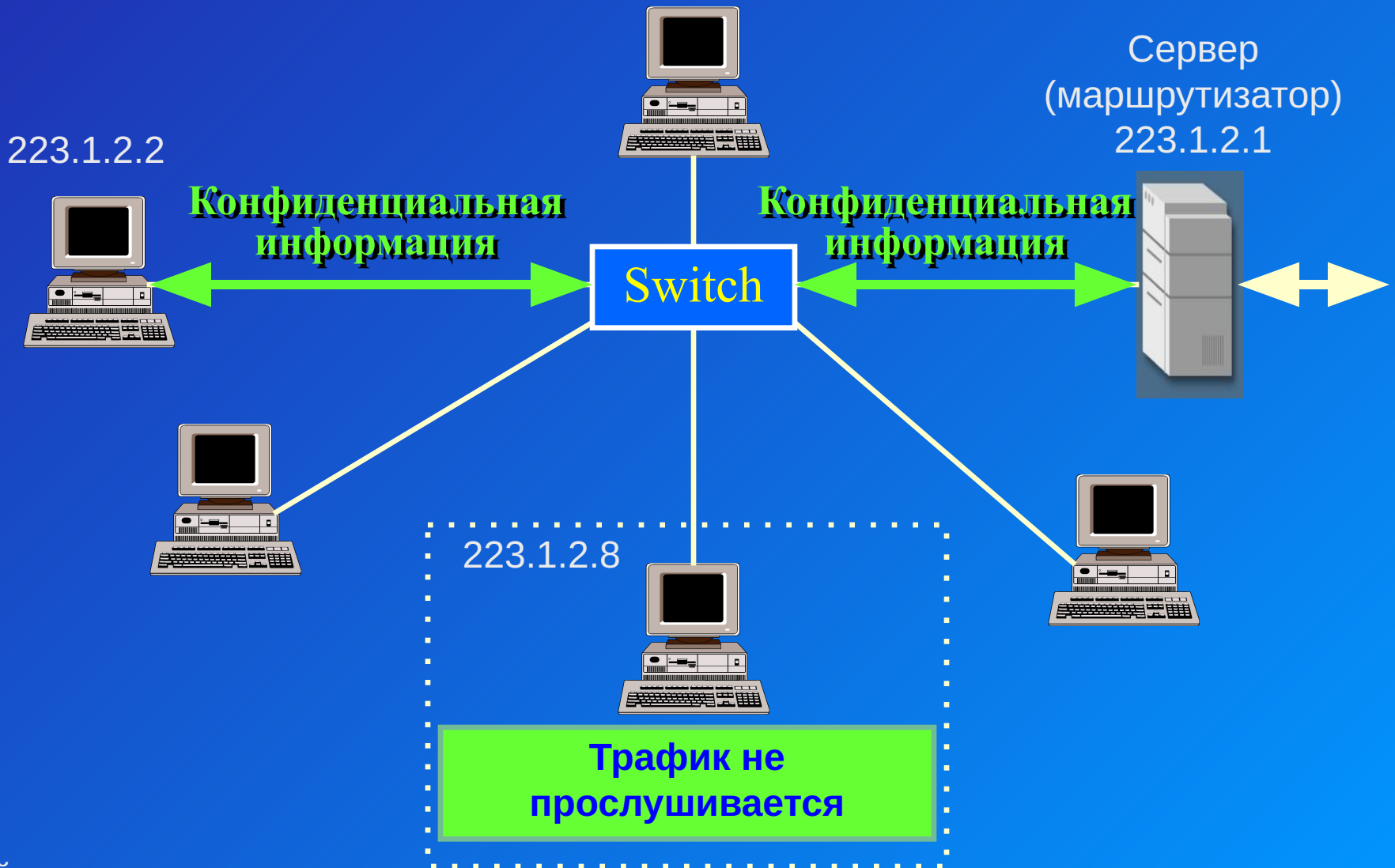
16

31

Тип сети		Тип исслед. протокола	
LNA	LPA	Тип действия	
MAC адрес отправителя=			
=несуществующий		IP-адрес отправителя=	
=223.1.2.1		MAC адрес получателя=	
=адрес объекта атаки			
IP-адрес получателя = адрес объекта атаки			

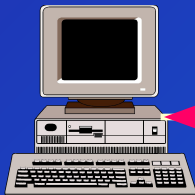
Нарушитель

ARP-spoofing



ARP-spoofing

223.1.2.2



**ARP ответ
к 223.1.2.2**

Switch

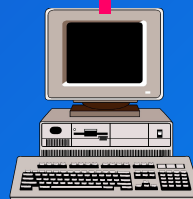
Сервер
(маршрутизатор)
223.1.2.1



```
C:\>arp -a
```

```
Interface: 223.1.2.2 on Interface 0x1000003
```

Internet Address	Physical Address	Type
223.1.2.1	00-66-66-66-66-66	dynamic

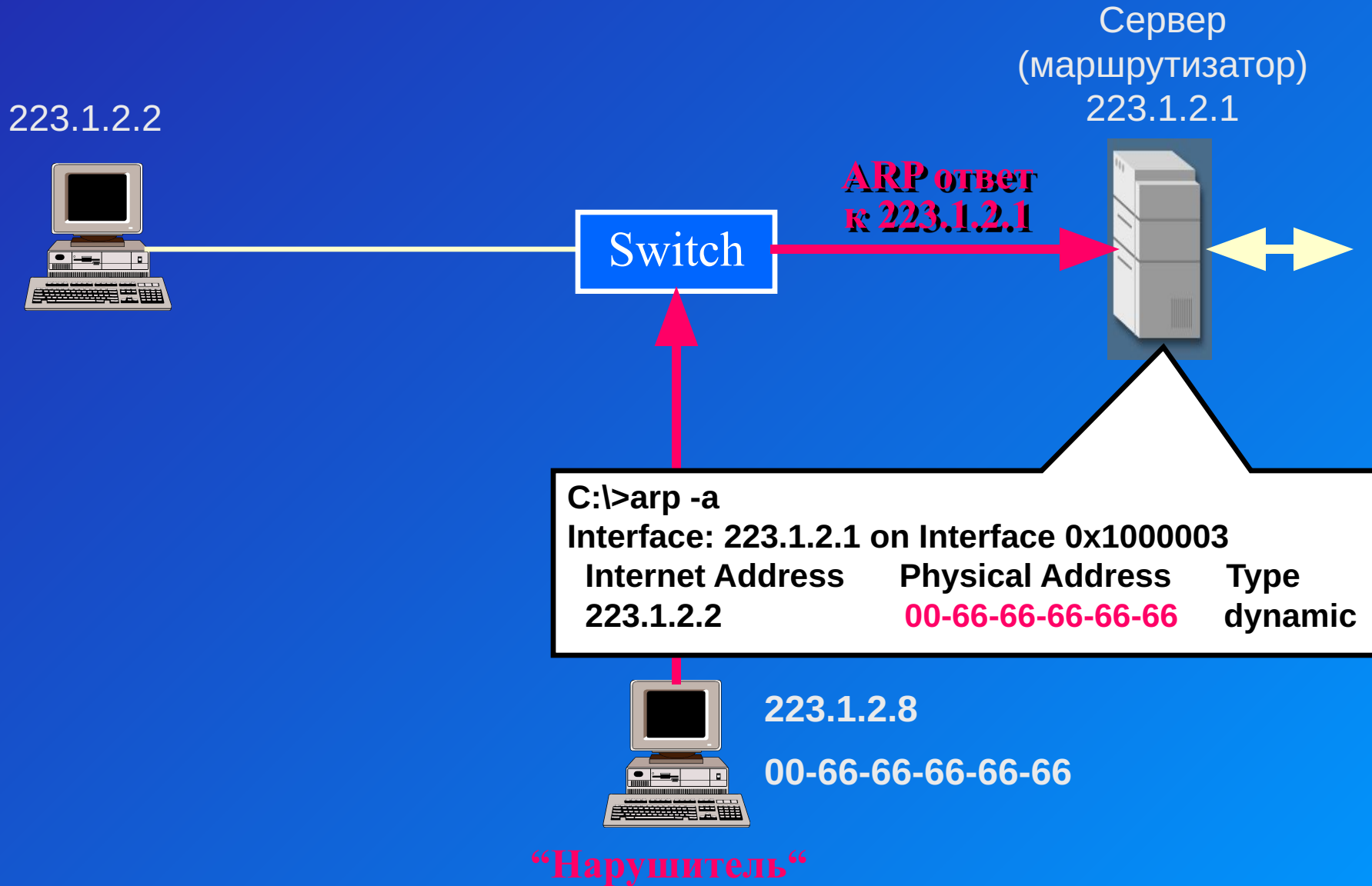


223.1.2.8

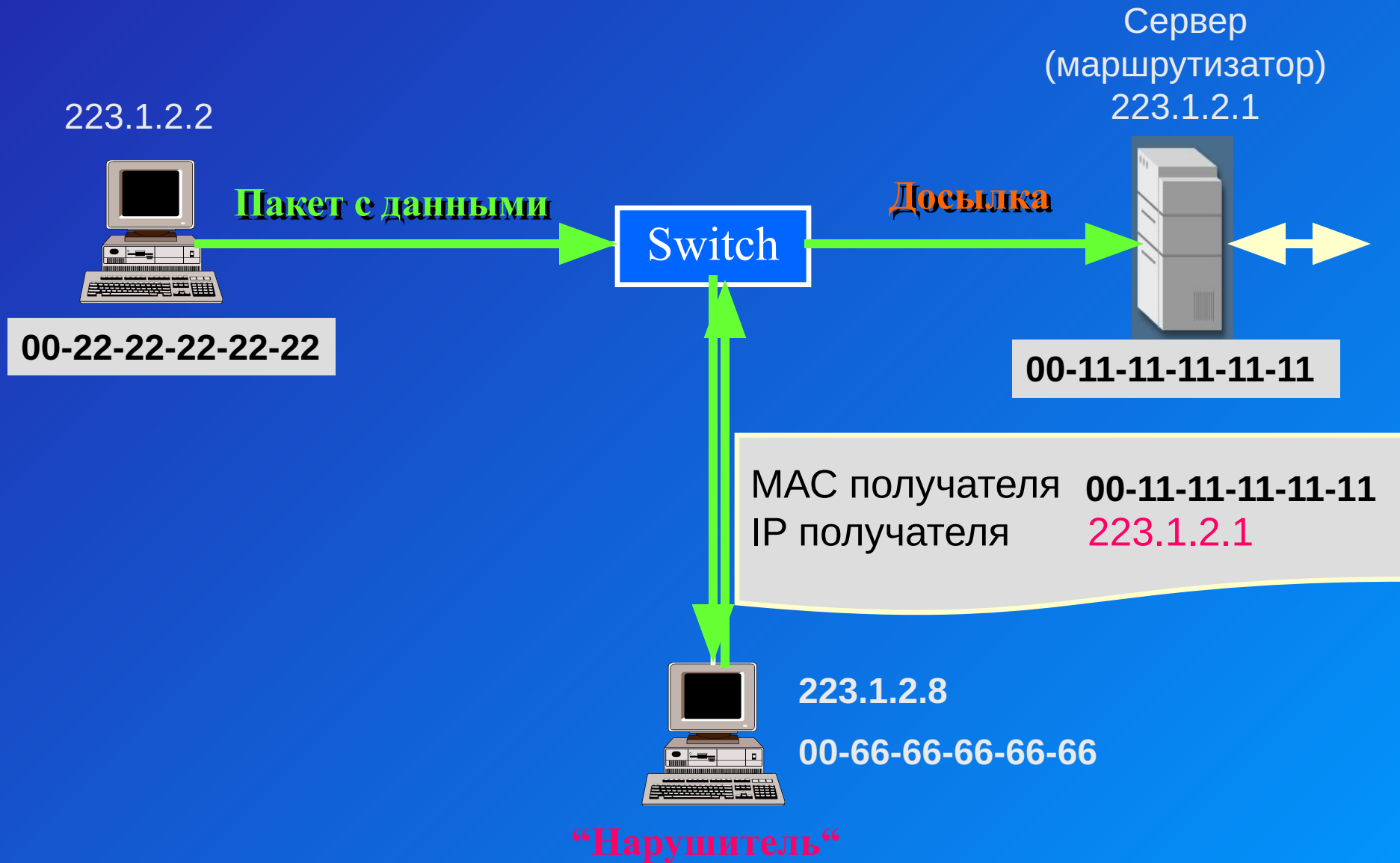
00-66-66-66-66-66

“Нарушитель”

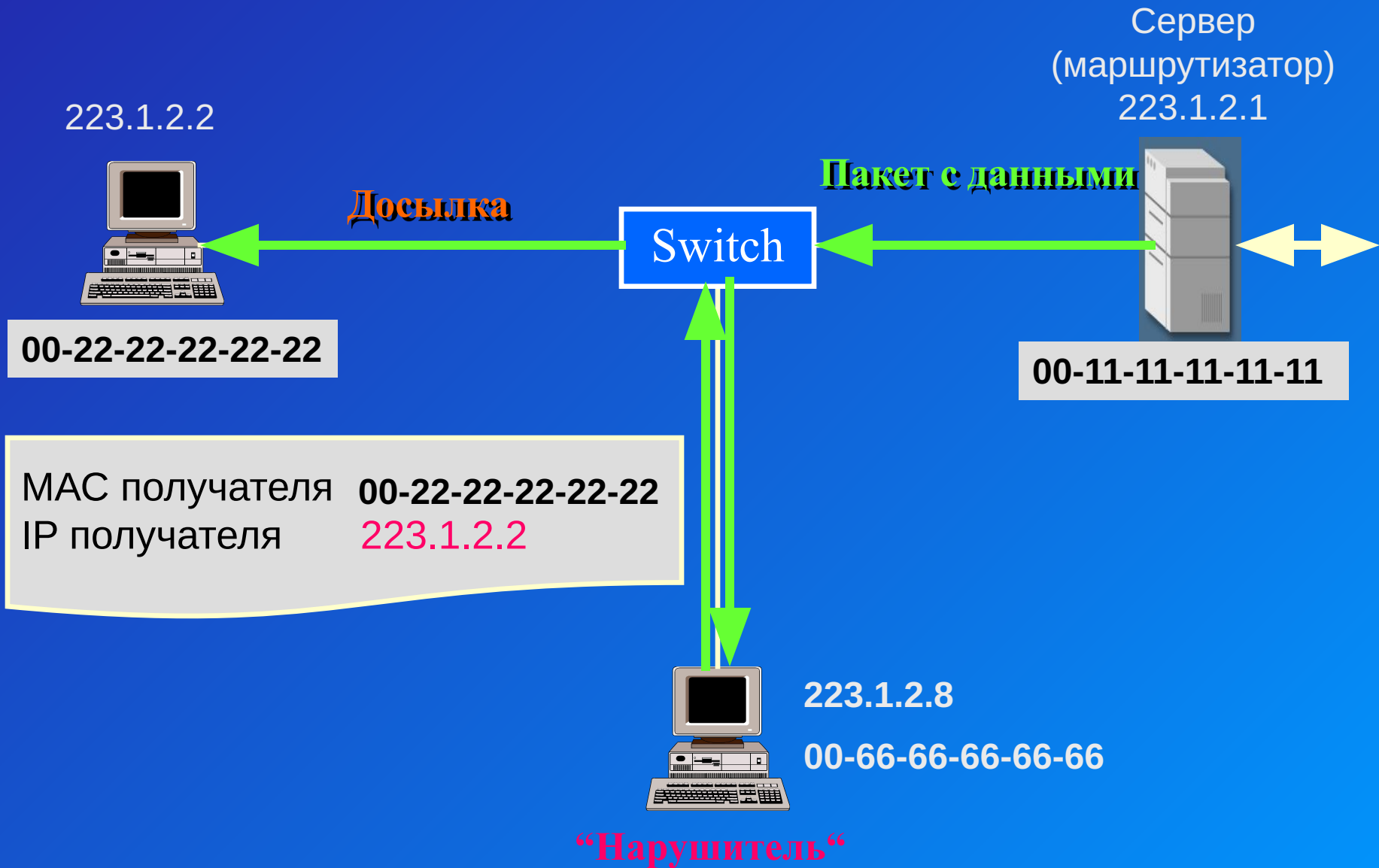
ARP-spoofing



ARP-spoofing



ARP-spoofing

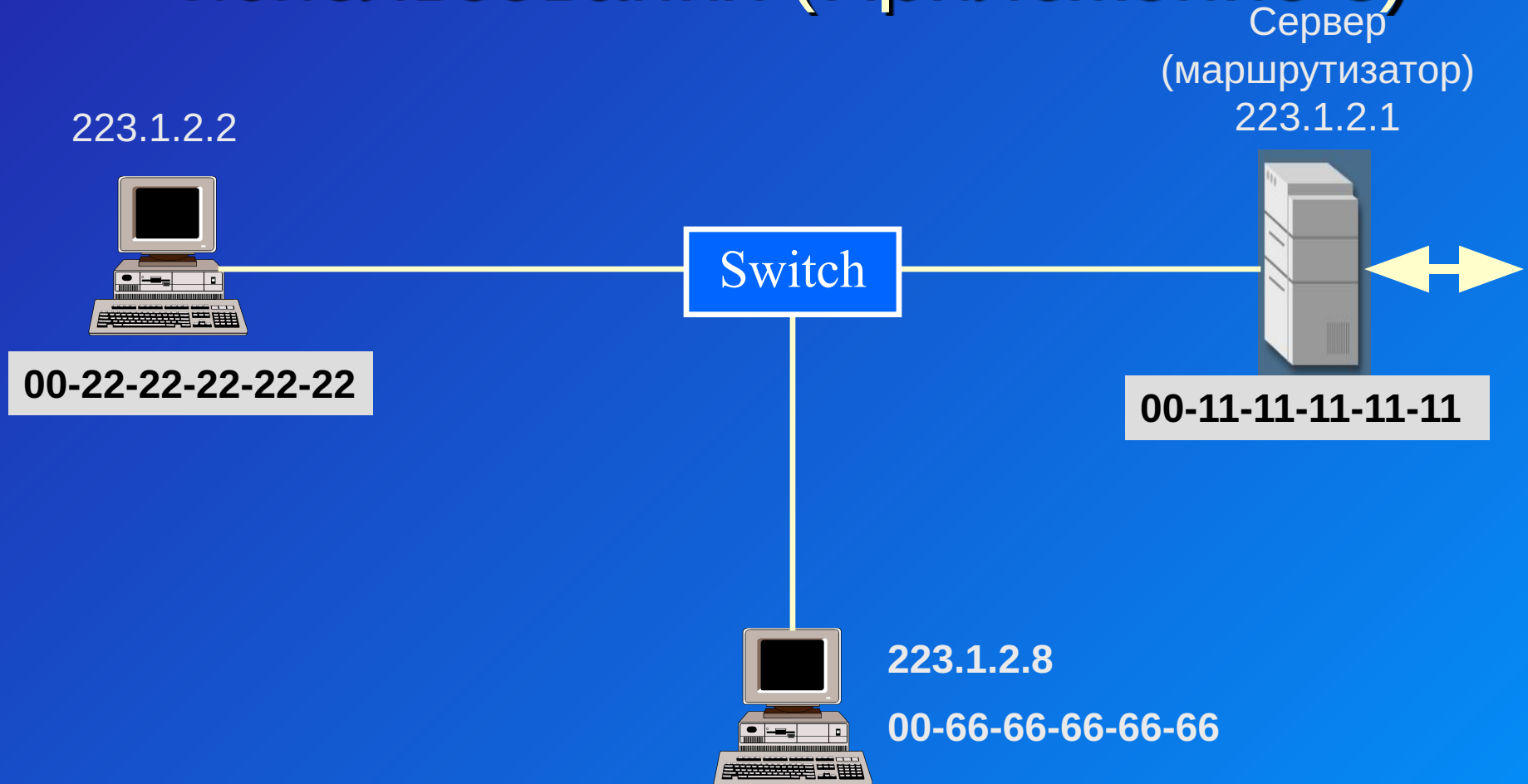


Программа ettercap

- IP BASED SNIFFING
- MAC BASED SNIFFING
- ARP BASED SNIFFING
- PUBLIC ARP
- SMART PUBLIC ARP

Методы анализа трафика

Программа ettercap – пример использования (Приложение 3)



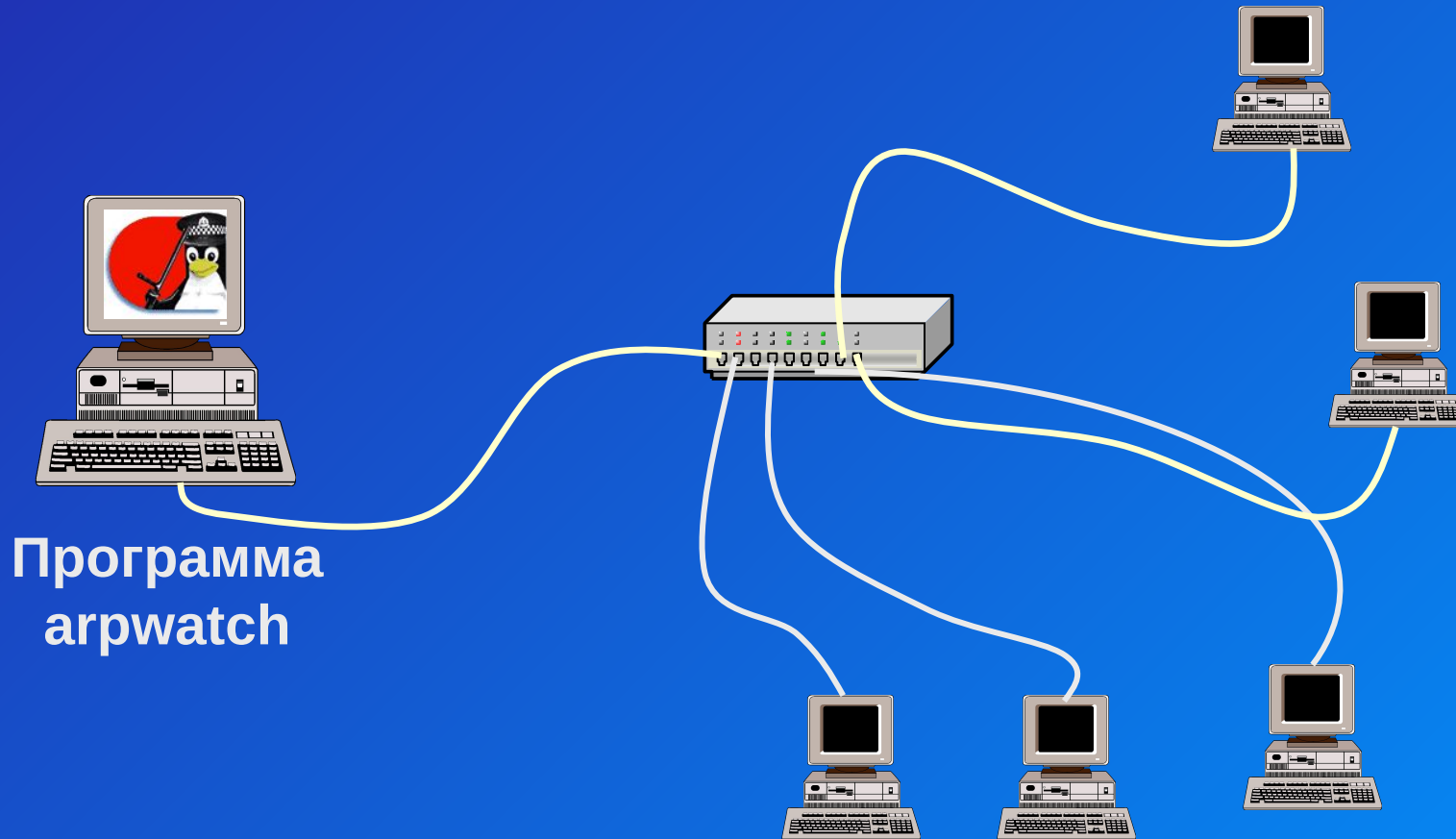
Узел нарушителя:

- Программа «ettercap»
- Network Monitor (или другой сетевой анализатор)

Меры защиты

- Ведение таблицы соответствия MAC и IP адресов
- Использование статических записей в ARP-таблице (кроме Windows)
- Использование персональных МЭ с поддержкой фильтрации ARP-пакетов
- Поиск нарушителя – внутри сегмента

Программа arpwatch



Программа
arpwatch

Изменение алгоритма работы ARP



OS Linux

- Сопоставление полученного ARP-ответа с имеющимся MAC-адресом
- Восприятие ответа только при посылке запроса

Практическая работа 3

- Основные приёмы работы с ARP
- Изучение некорректного ARP-запроса
- ARP-spoofing
- Программа arpswatch