Физический и канальный уровни

Раздел 2 – Тема 5

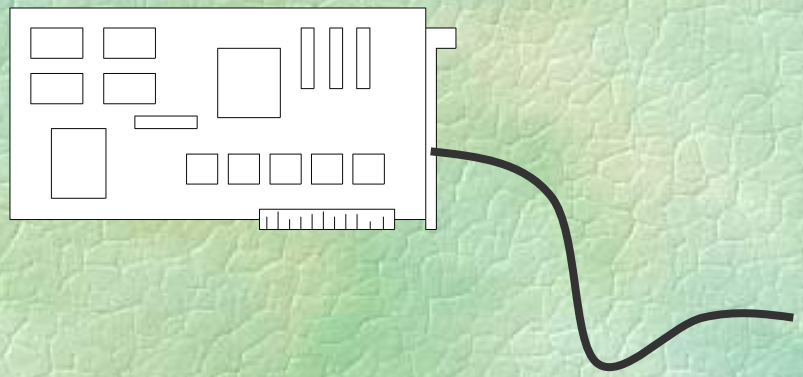
Физический и канальный уровни

Сетевой уровень

Канальный уровень

Физический уровень

Драйвер NIC



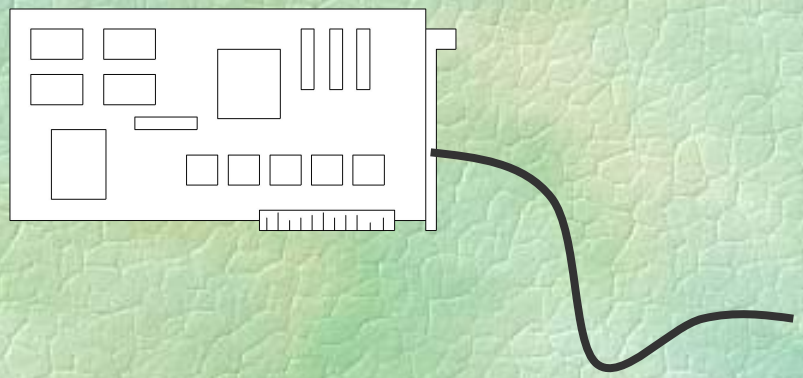
Физический и канальный уровни для различных технологий

Уровни OSI	Технология ATM	Технология X25	Технология Ethernet	Технология Frame Relay
Канальный	Уровень ATM	Протокол LAP-B	LLC/MAC	Протокол LAP-F
Физический	Подуровни TC/PM (стандарты ANSI T1.624)	X21, X21bis	Спецификации физического уровня	Интерфейсы BRI и PRI

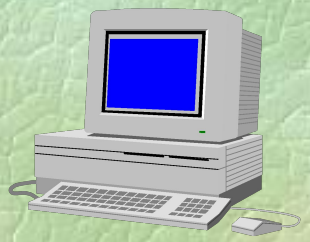
Подуровни LLC и MAC

<table>
<tr><td colspan="2">Сетевой уровень</td></tr>
<tr><td rowspan="2">Канальный уровень</td><td>LLC</td></tr>
<tr><td>MAC</td></tr>
<tr><td colspan="2">Физический уровень</td></tr>
</table>

Драйвер NIC

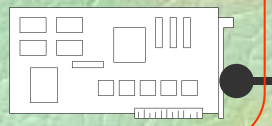


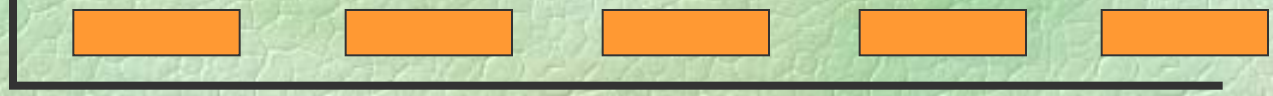
Фреймы



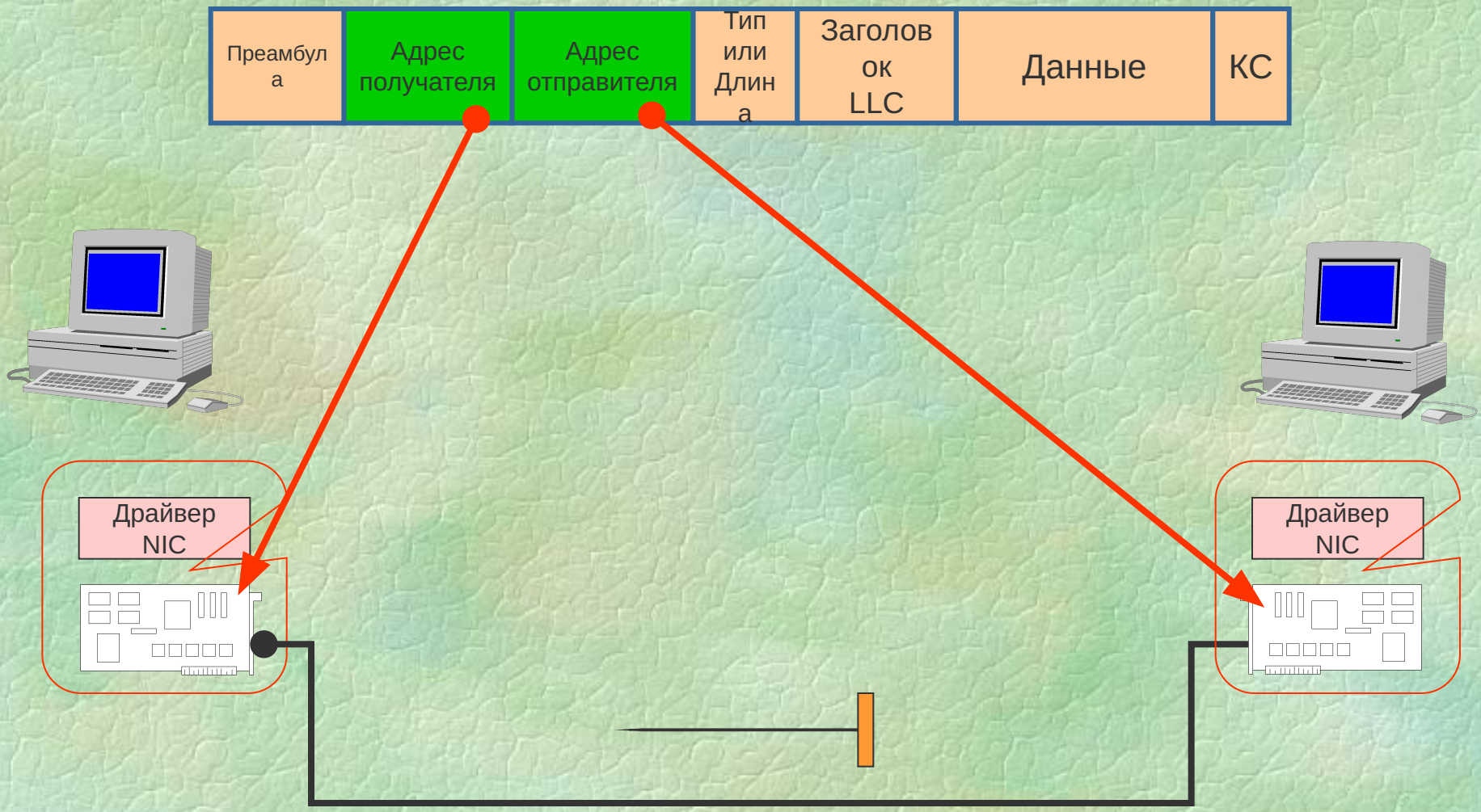
Преамбула	Адрес получателя	Адрес отправителя	Тип или Длина	Заголовок LLC	Данные	КС
8	6	6	2			4

Драйвер NIC





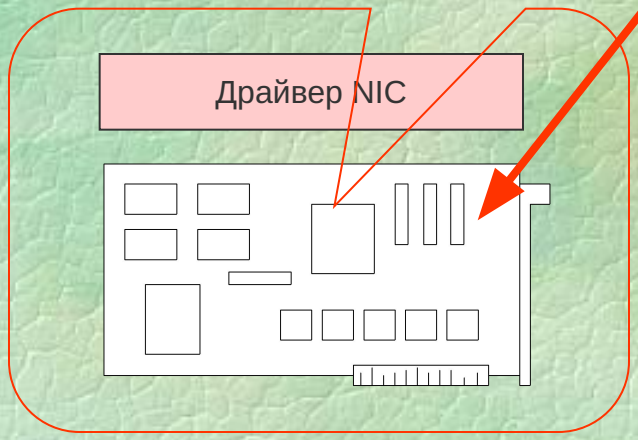
Адресация на канальном уровне



MAC-адрес

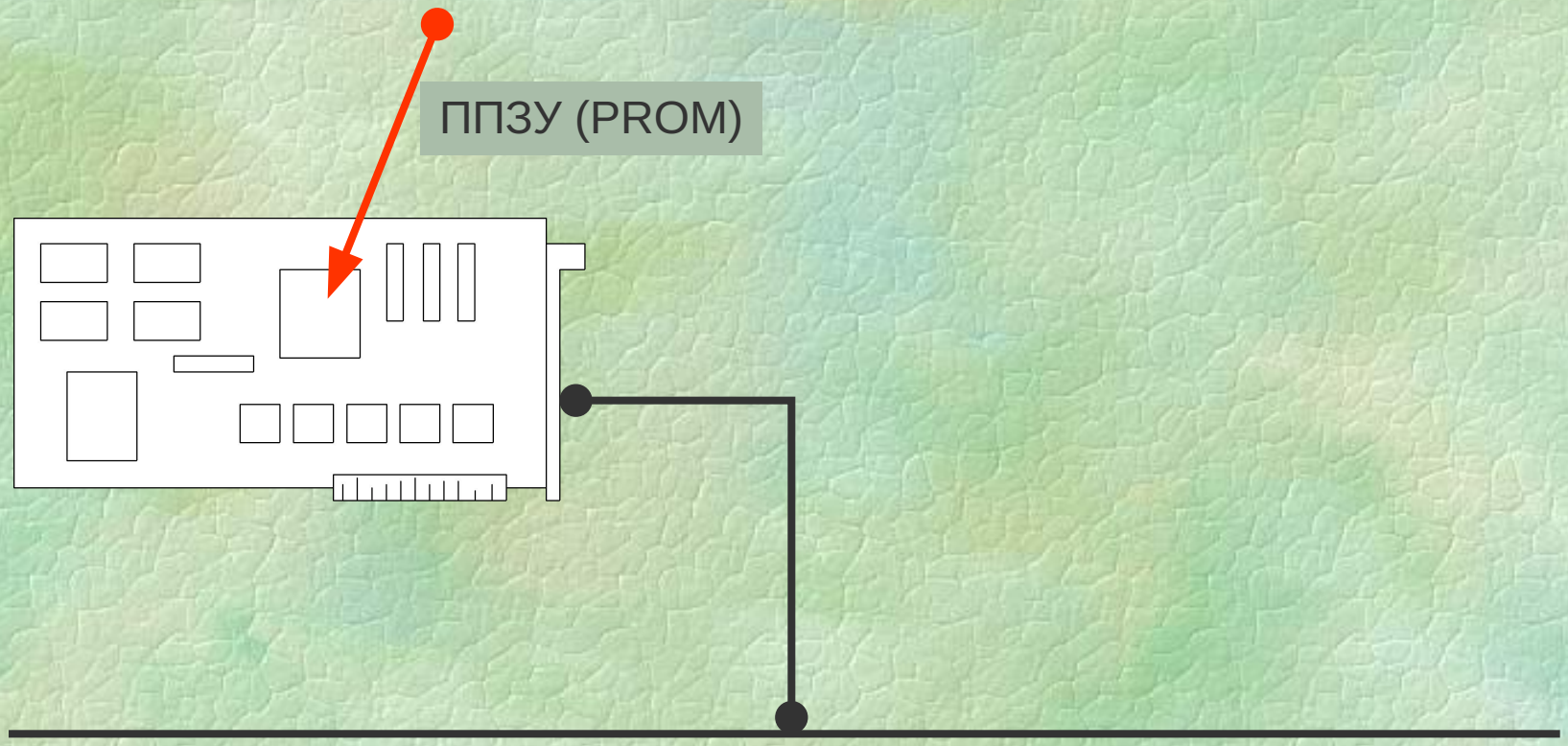
Преамбула	Адрес получателя	Адрес отправителя	Тип или Длина	Заголовок LLC	Данные	КС

0	0	Идентификатор производителя (22 бита)	Адрес узла (24 бита)



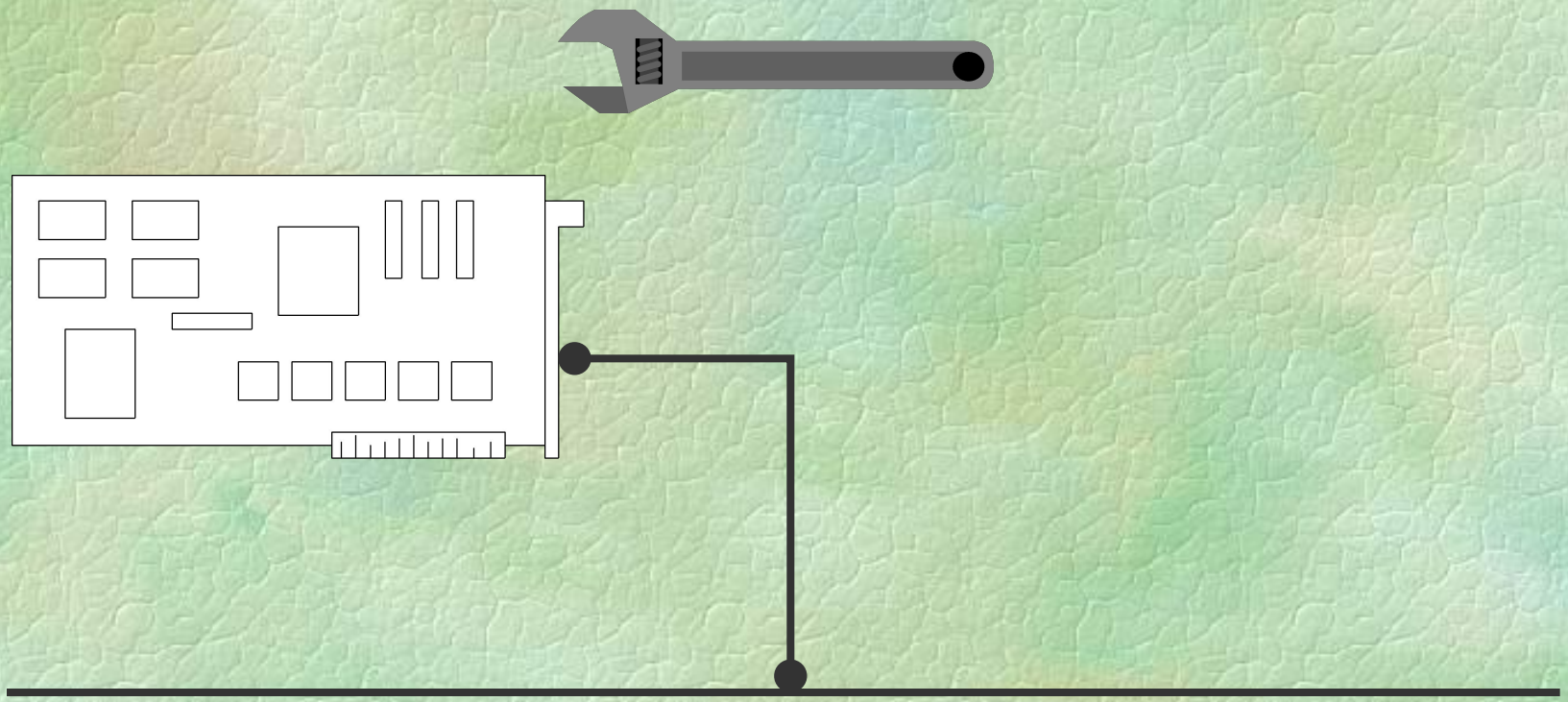
MAC-адрес и разграничение доступа

0	0	Идентификатор производителя (22 бита)	Адрес узла (24 бита)



Изменение MAC-адреса (MAC Address Spoofing)

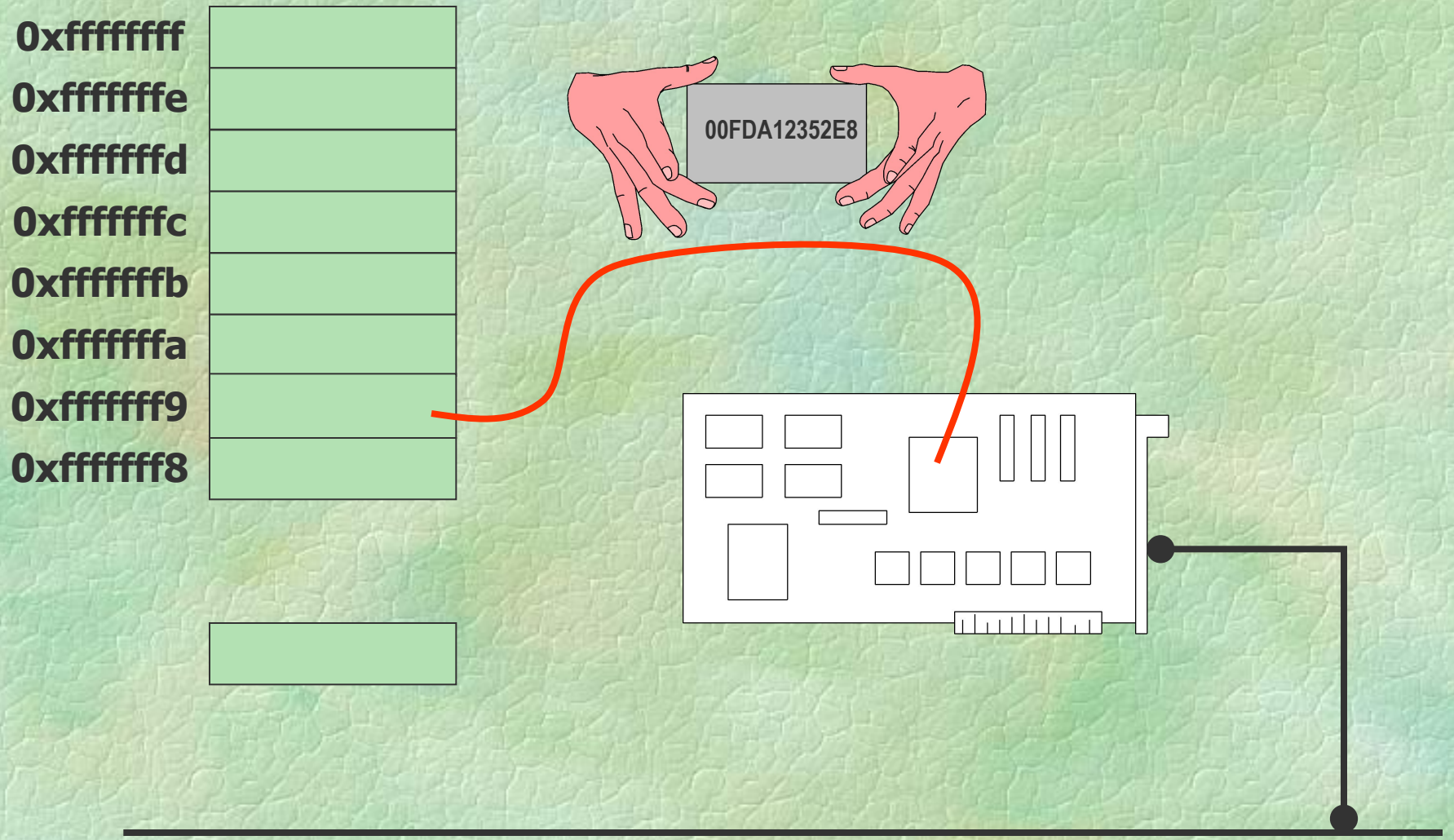
- На физическом уровне (перепрошивка)
- В момент считывания в память ОС
- На уровне ОС



Изменение MAC-адреса на физическом уровне

«Перепрошивка»

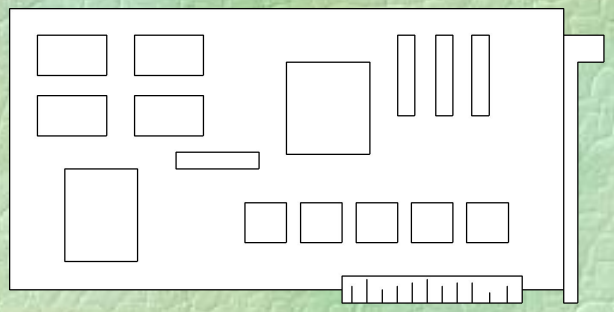
Изменение MAC-адреса в момент считывания в память ОС



Изменение MAC-адреса на уровне ОС

ОС Windows:
Значимый элемент реестра «NetworkAddress»

Windows NT:
Ключ
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<сетевой адаптер>\Parameters
Значимые элементы
NetworkAddress="xx-xx-xx-xx-xx-xx"
SelectedID="xx-xx-xx-xx-xx-xx"



Практическая работа 1
Изменение MAC-адреса в среде Windows 2000

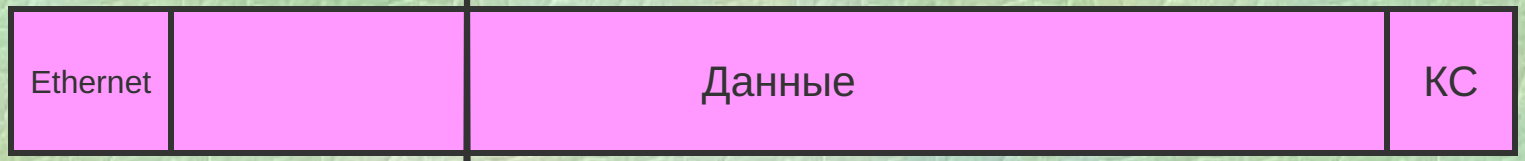
- Редактирование свойств сетевого адаптера
- Редактирование реестра
- Использование программы CMAC

Выводы: когда требуется изменение MAC-адреса

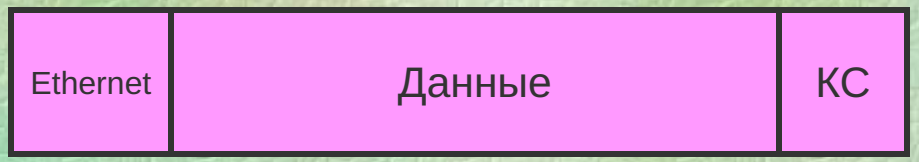
- Тестирование систем на наличие уязвимостей аутентификации и авторизации на основе MAC-адресов.
- Резервирование узлов, при котором требуется точное совпадение имени, IP-адреса и MAC-адреса. При этом не требуется обновление ARP-таблиц узлов при вводе в строй резервного узла
- Разрешение проблем, связанных с маршрутизацией, работой протокола ARP и т. д.
- Тестирование систем обнаружения атак
- Установка приложений, привязанных к MAC-адресам
- Замена сетевого адаптера
- Подключение к кабельному модему (многие провайдеры услуг Интернет при выдаче IP-адреса по DHCP производят проверку MAC-адреса).

Размер кадра Ethernet

1500 байт - максимум



46 байт - минимум



Заполнитель

Описание уязвимости

Номер

Описание

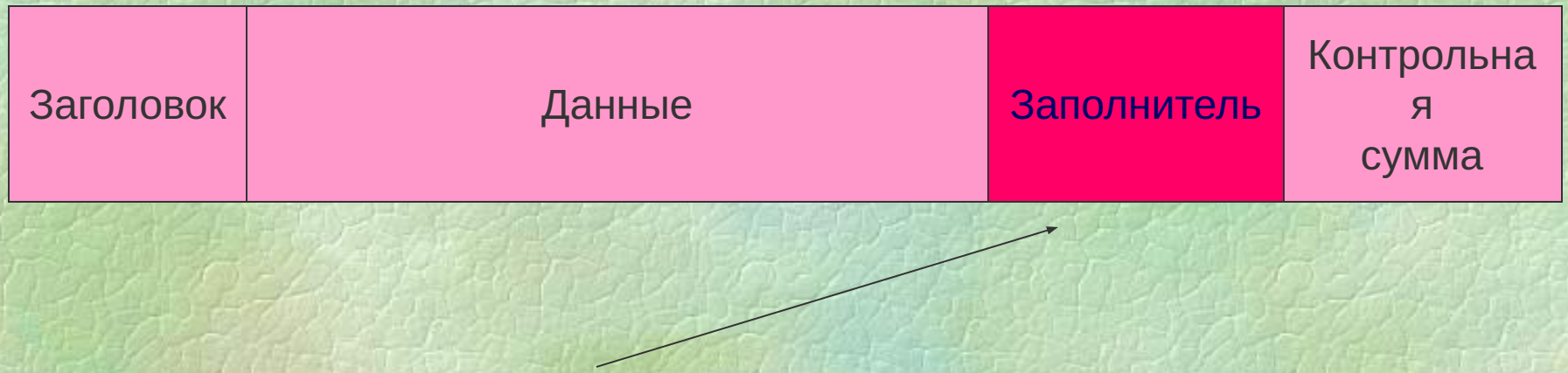
CAN-2003-0001

Multiple ethernet Network Interface Card (NIC) device drivers do not pad frames with null bytes, which allows remote attackers to obtain information from previous packets or kernel memory by using malformed packets, as demonstrated by Etherleak

(Многие драйверы сетевых адаптеров не используют в качестве заполнителя нулевые байты, что позволяет нарушителю получить содержимое памяти ядра или предыдущих пакетов)

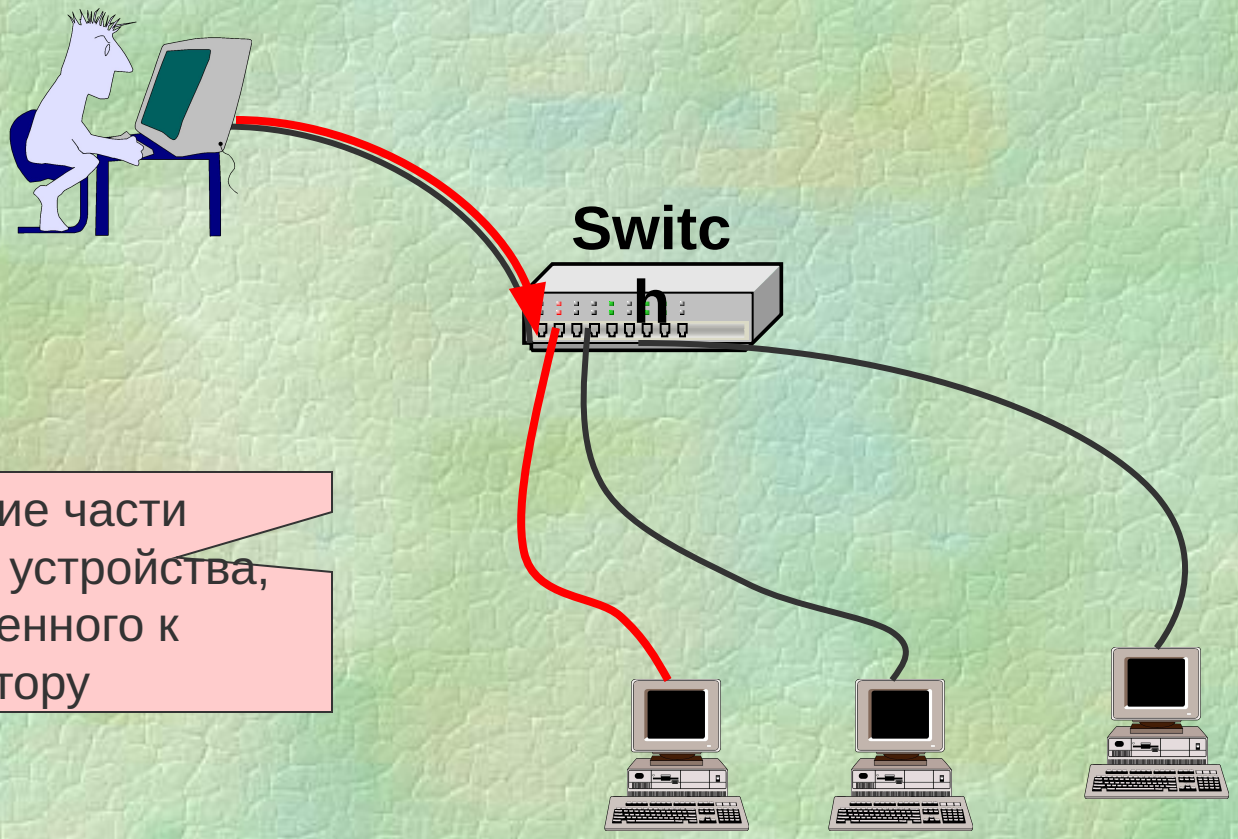
Содержимое заполнителя

46



- Dynamic kernel buffer (динамическая память ядра)
- Static device driver buffer (буфер драйвера сетевого адаптера)
- Hardware device transmit buffer (буфер сетевого адаптера)

Использование уязвимости



Получение части трафика устройства, подключенного к коммутатору

Тестирование на наличие уязвимости

Ping <тестируемый узел> -l 1
(ICMP – эхо запрос размером 1 байт)

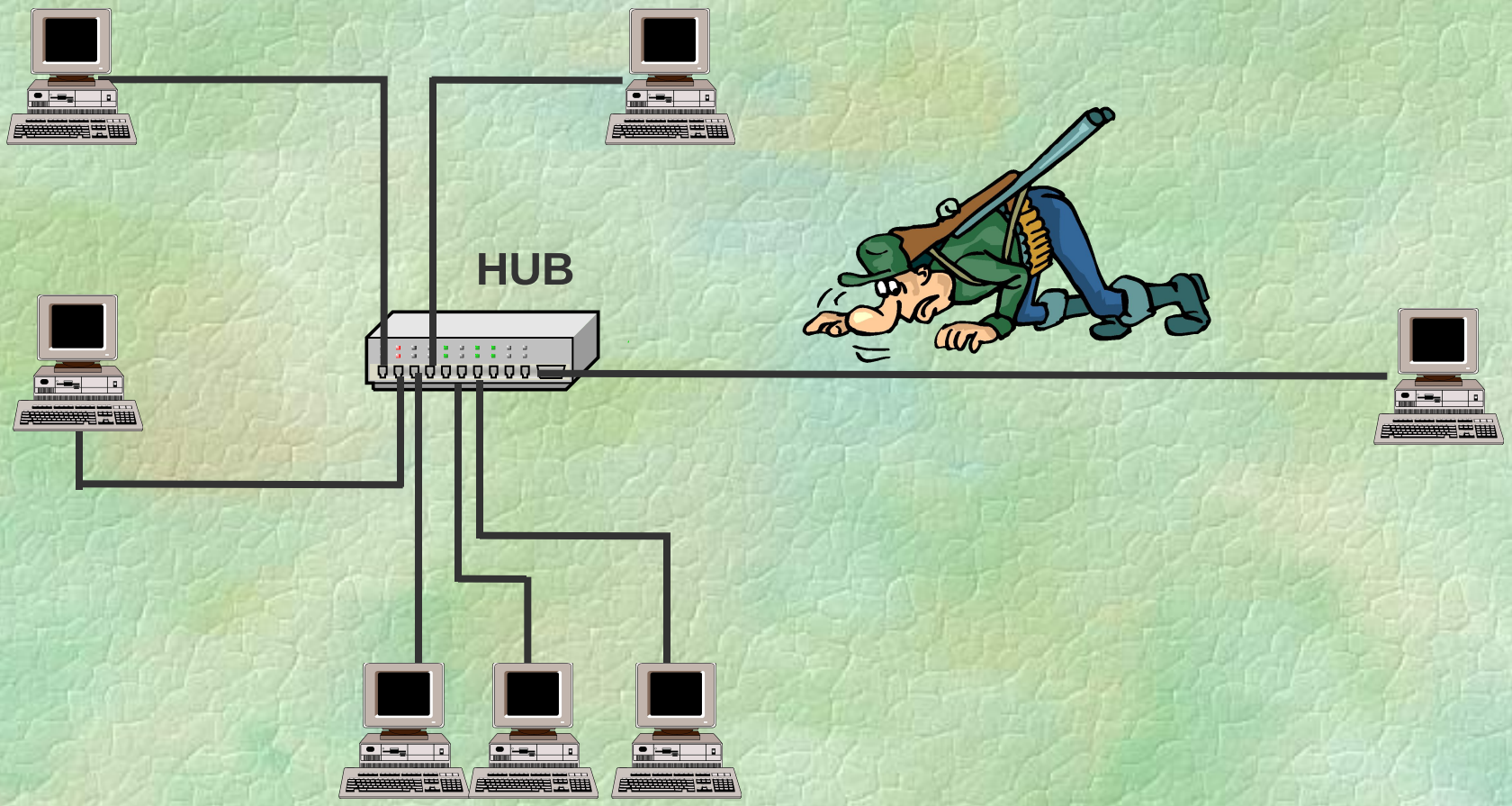
Драйверы из состава Windows 2003 Server

Name: Etherleak information leak in Windows Server 2003 drivers
Systems Affected: Windows Server 2003 (all versions)
Severity: Low/Medium Risk
Vendor URL: http://www.microsoft.com/windowsserver2003/
Author: Chris Paget (chrisp@ngssoftware.com)
Date: 9th June 2003Advisory
URL: http://www.nextgenss.com/advisories/etherleak-2003.txt
Advisory number: #NISR09062003

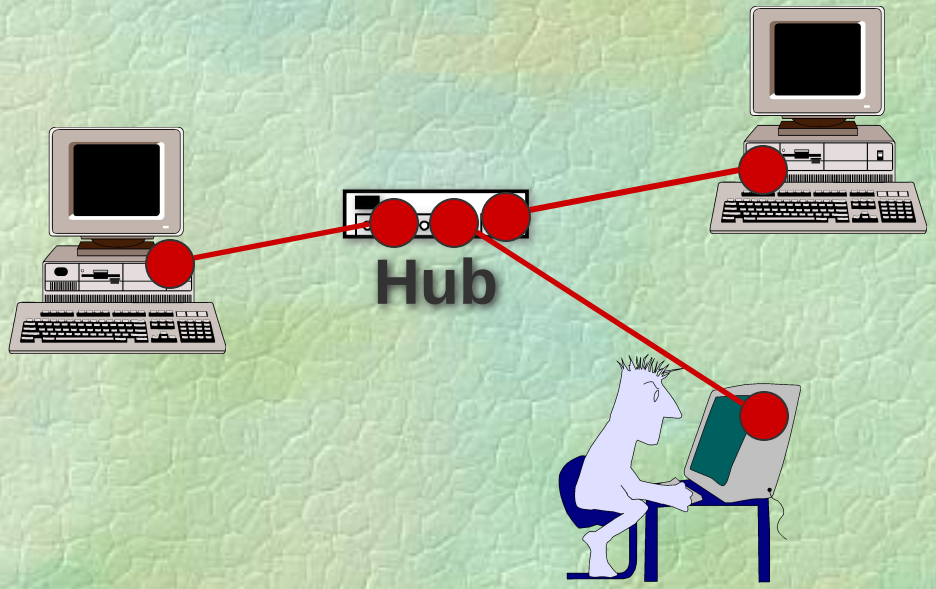
Уязвимые драйверы:

- VIA Rhine II Compatible (интегрированные с материнскими платами)
- AMD PCNet family (используются отдельными версиями VMWare)

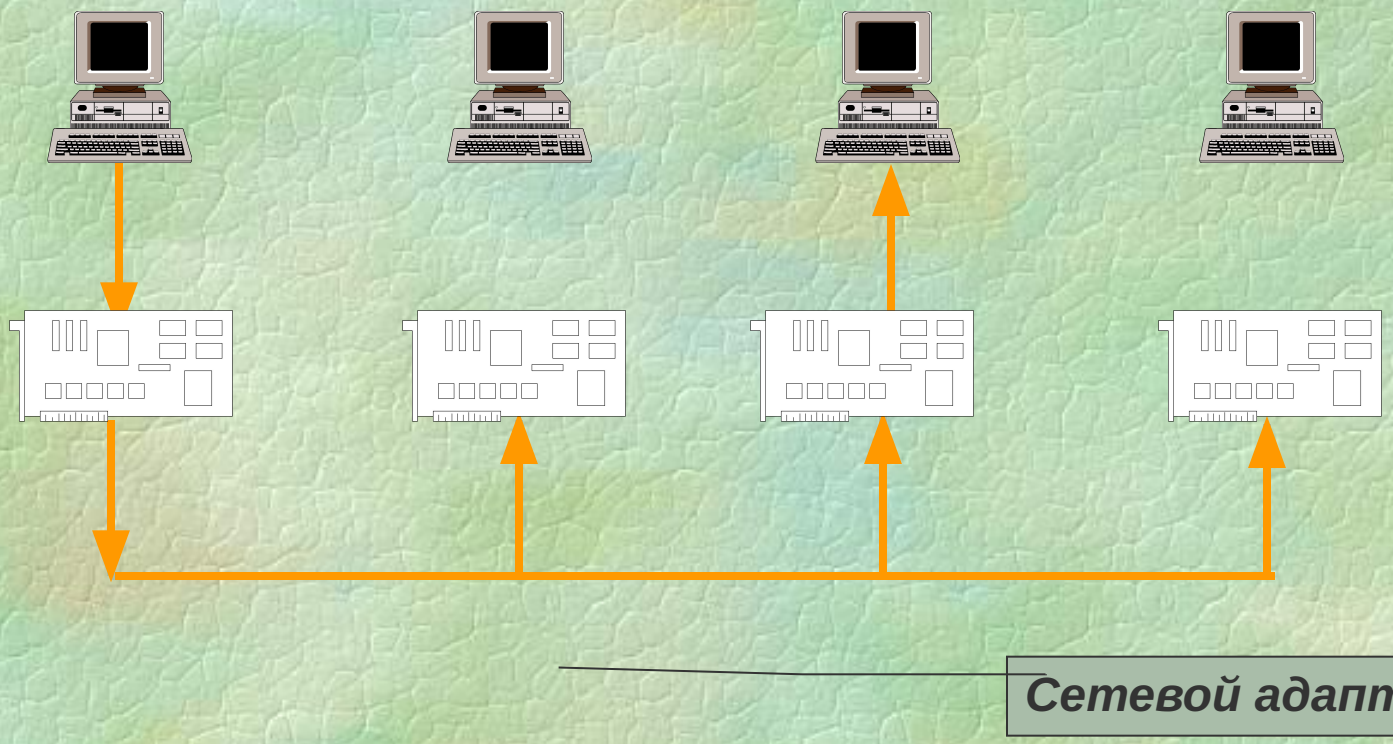
Сетевые анализаторы («снифферы»)



Сетевые анализаторы («снифферы»)



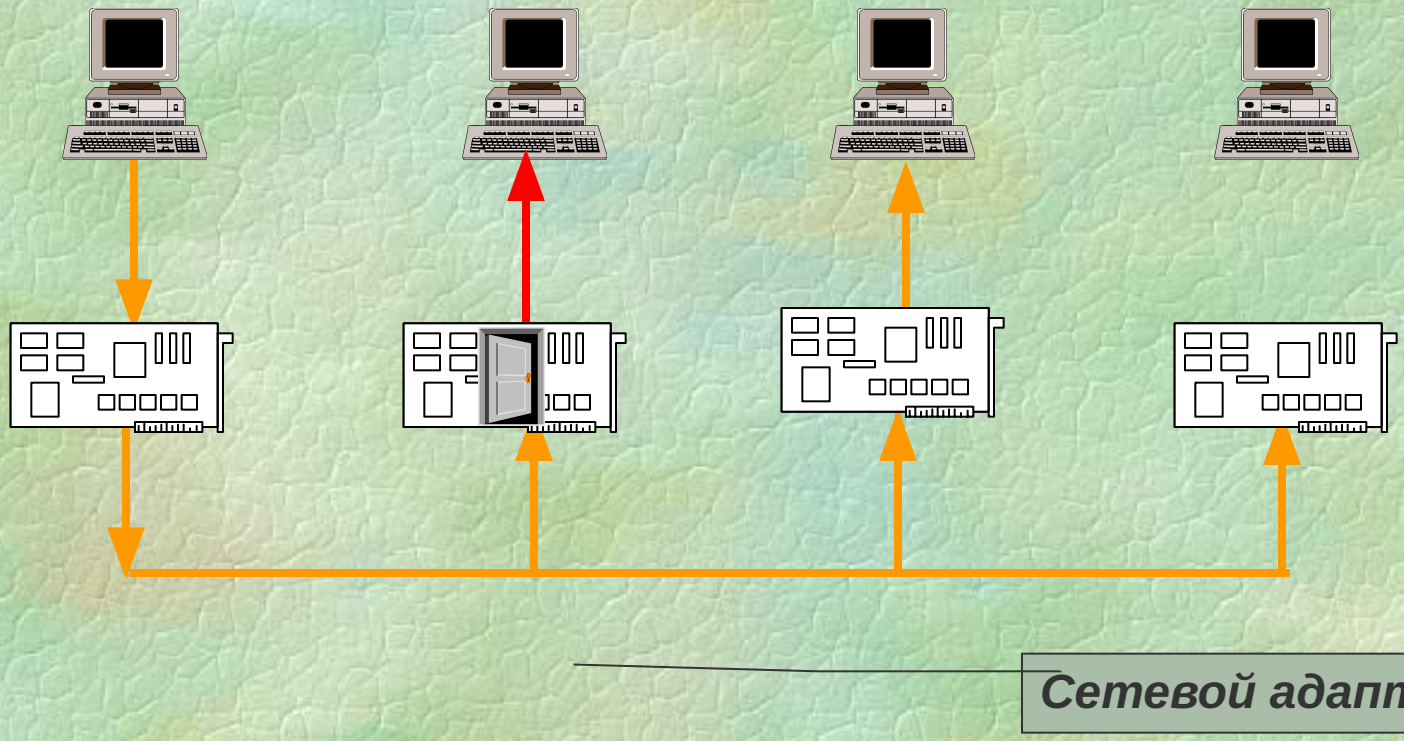
Селективный режим работы сетевого адаптера



Сетевые адаптеры фильтруют сообщения и не принимают те, которые не предназначены данному узлу

Такой режим работы сетевого адаптера называется селективным или режим non-promiscuous

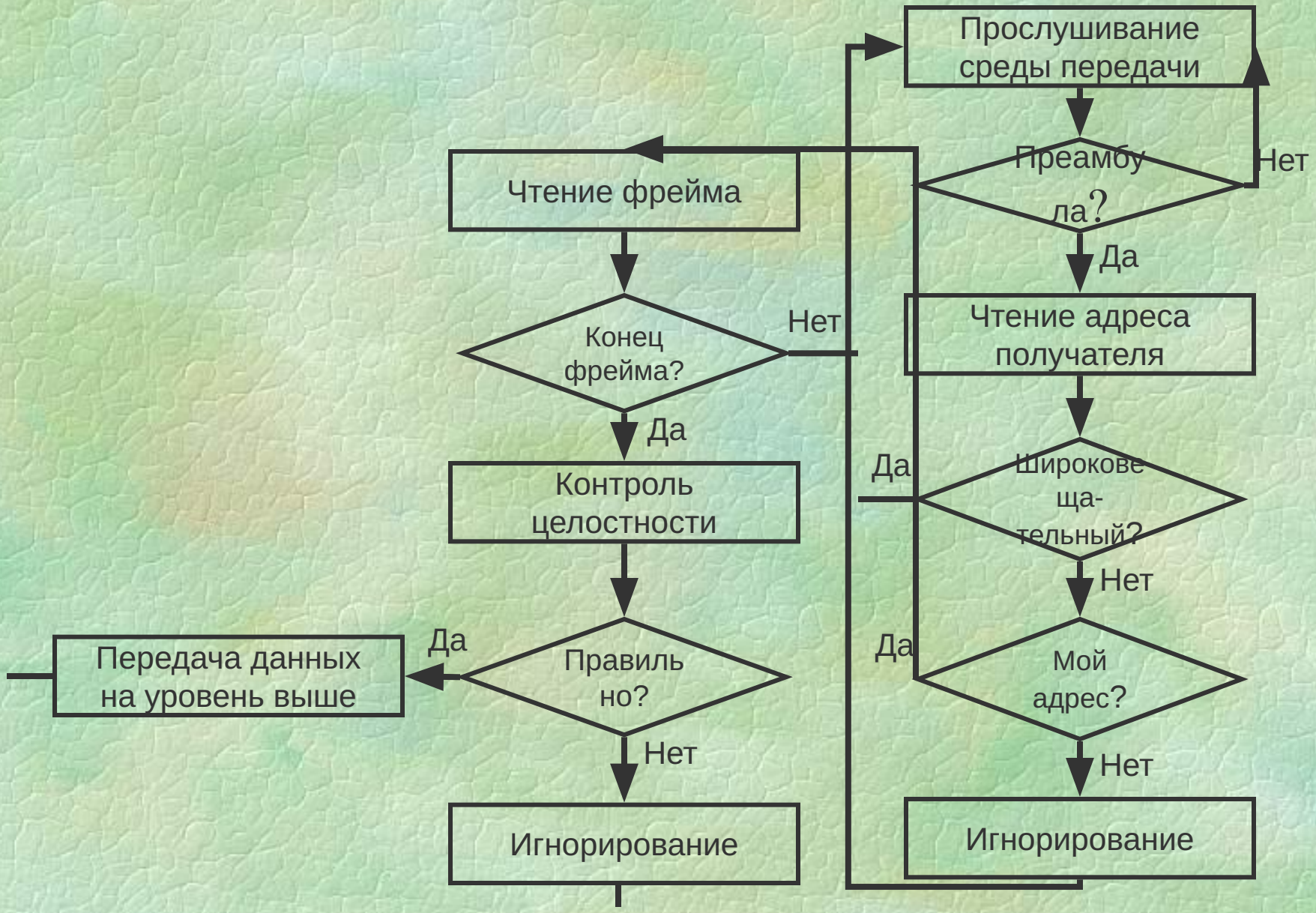
Неселективный режим работы сетевого адаптера



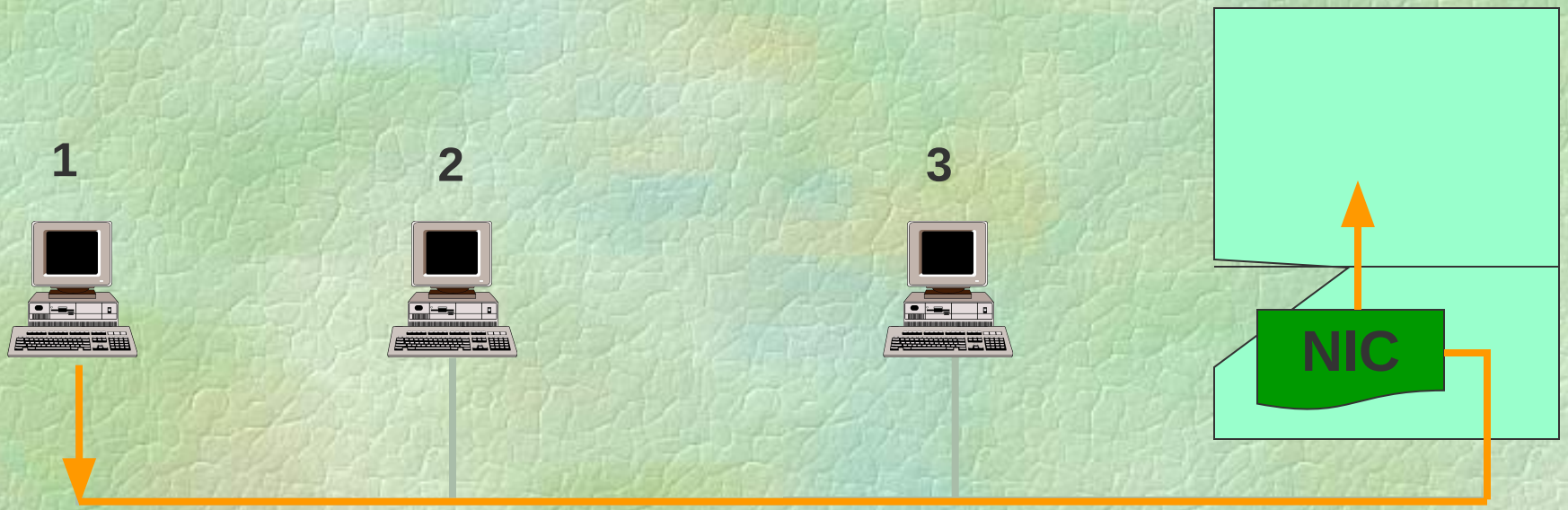
Однако если сетевой адаптер перевести в режим приёма всех проходящих сообщений, то в руках злоумышленника окажется весь сетевой трафик данного сегмента

Такой режим работы сетевого адаптера называется неселективным или promiscuous - режим

Процесс приёма данных



Селективный режим



- Адрес получателя совпадает с адресом узла

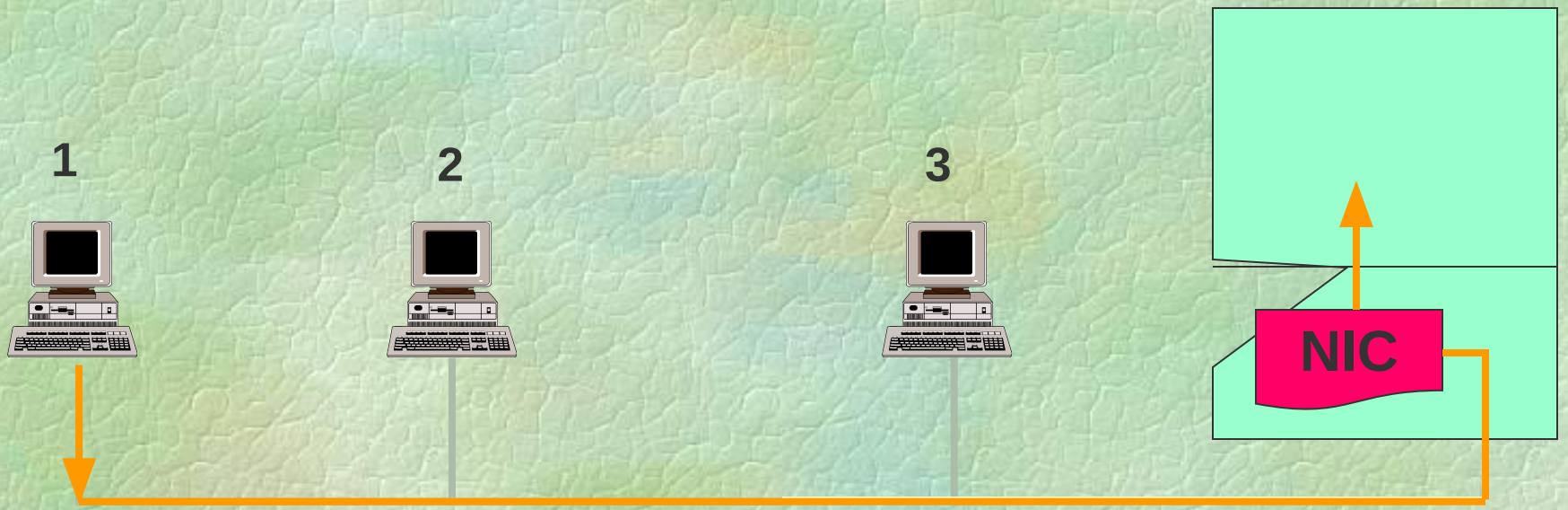
или

- Адрес получателя широковещательный

и

- Пакет прошёл проверку целостности

Неселективный режим



- Пакет прошёл проверку целостности

Сетевые анализаторы

- 

  SnifferPro
- **Microsoft Network Monitor (SMS)**
- **Real Secure Network Sensor**

Меры защиты

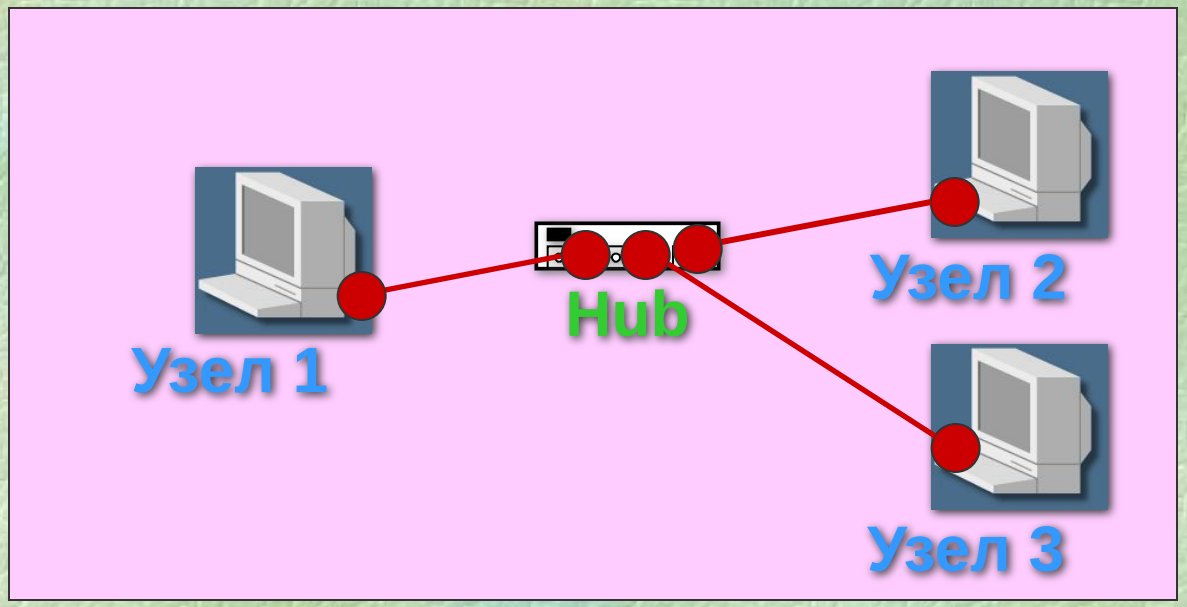
- Обнаружение снифферов

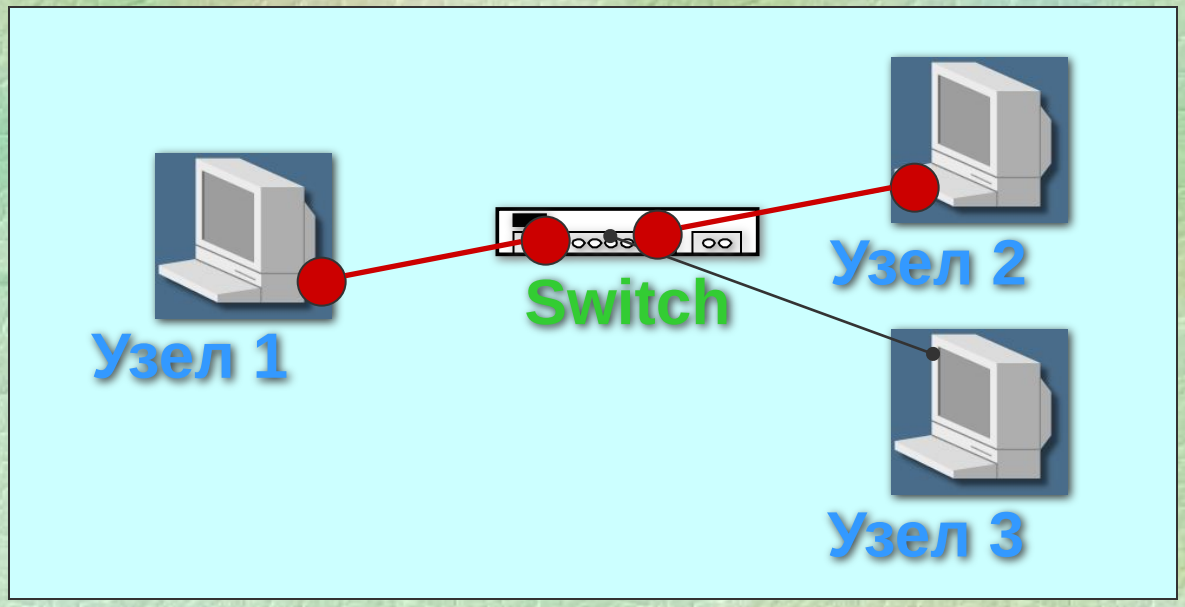
- Шифрование трафика

- Использование сетевых адаптеров, не поддерживающих неселективный режим

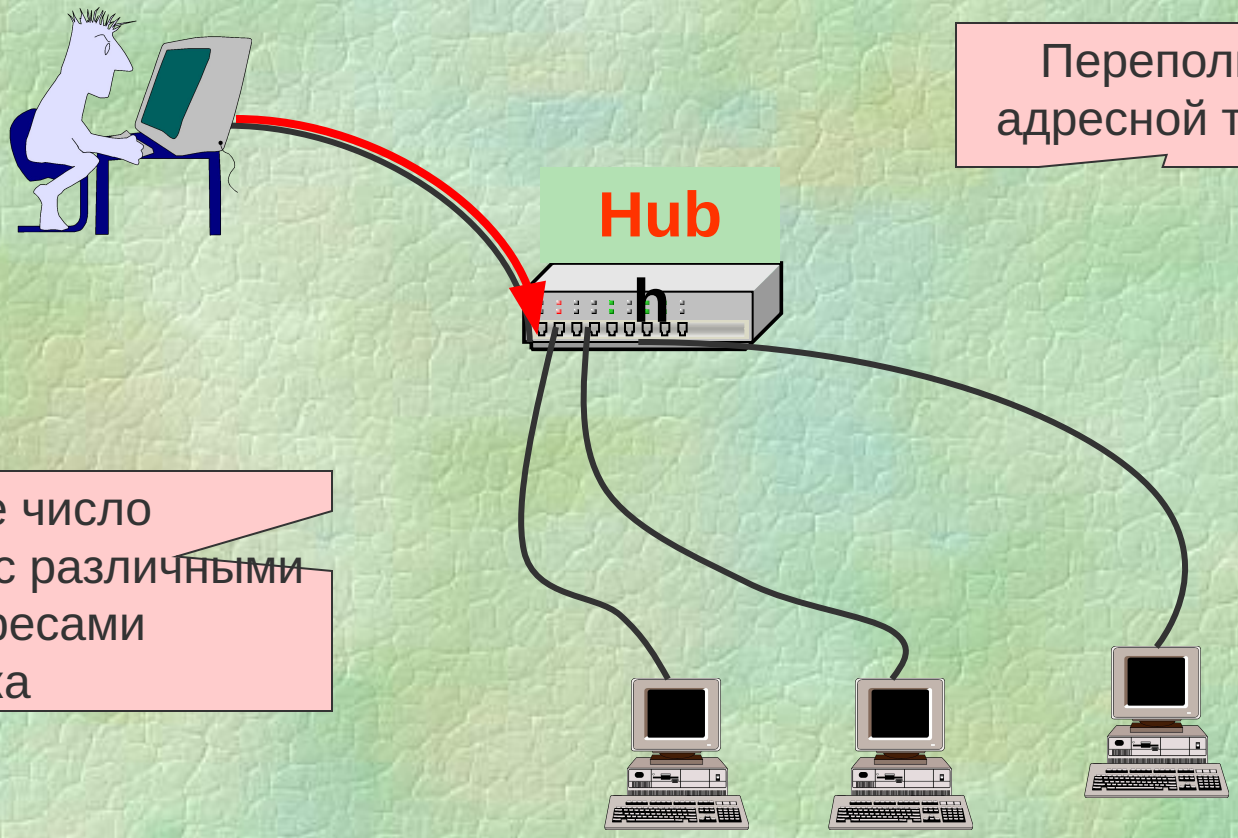
- Применение коммутаторов

Применение коммутаторов



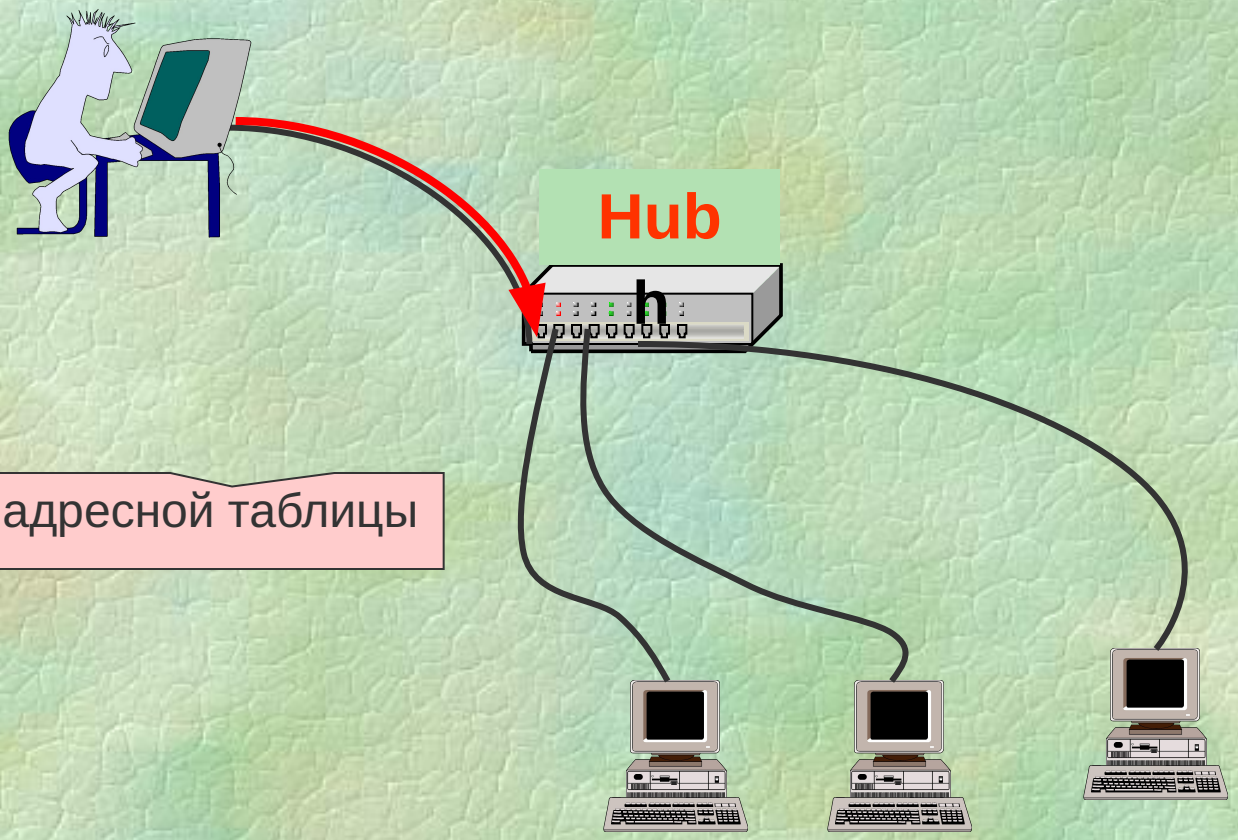


Уязвимости коммутаторов



Переполнение адресной таблицы

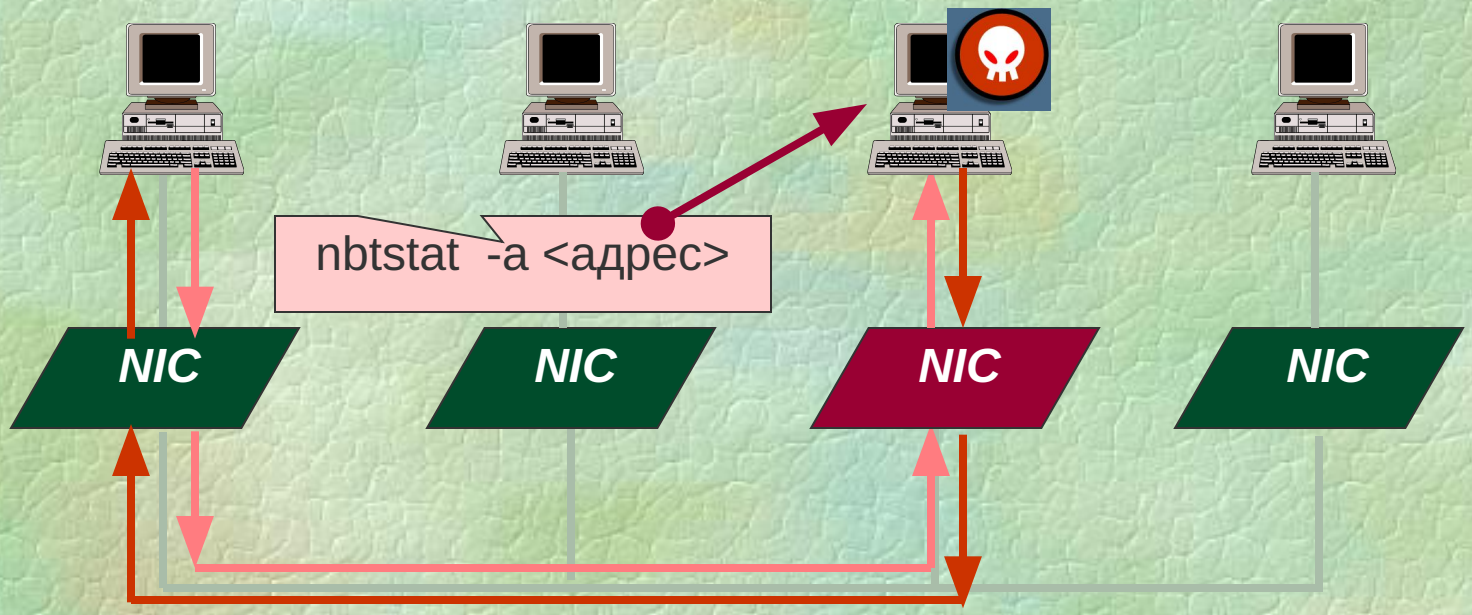
Уязвимости коммутаторов



Очистка адресной таблицы

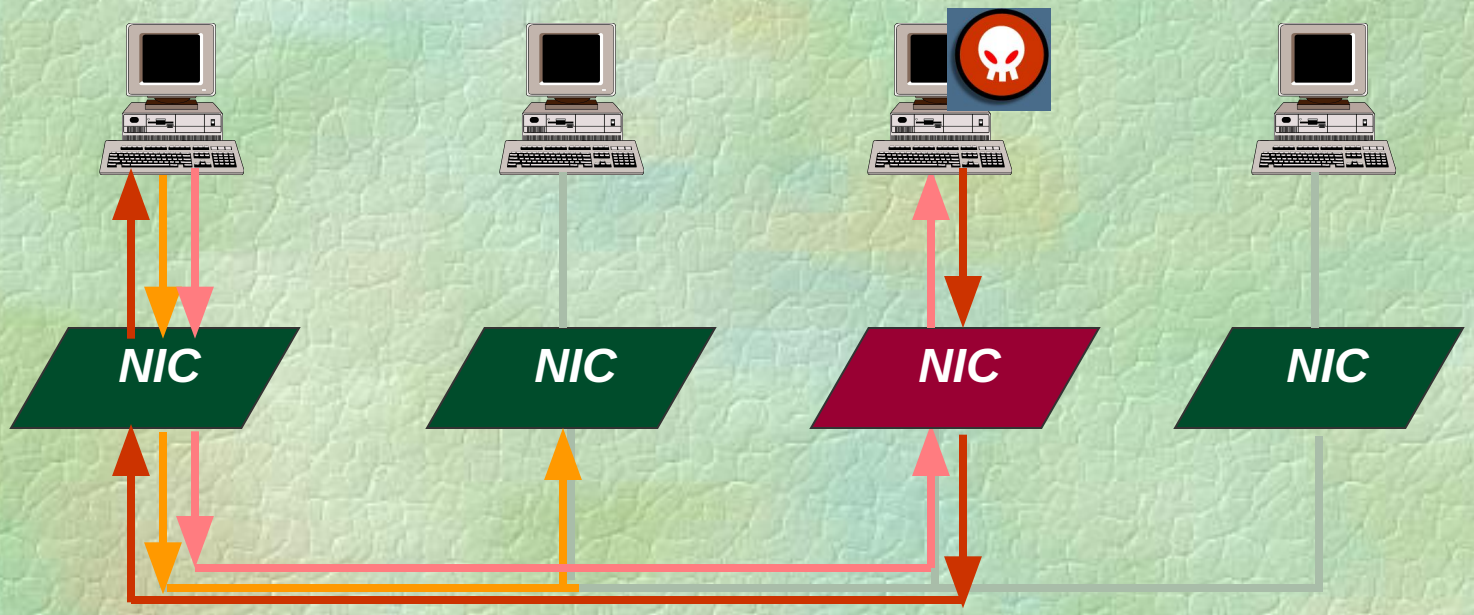
Очистка адресной таблицы

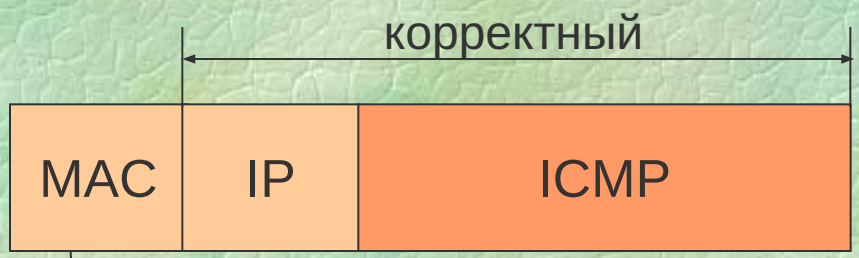
Обнаружение снифферов по косвенным признакам (Network Monitor)




```
 Name            Type        Status
---------------------------------------------
NT-IIS                <20>  UNIQUE     Registered
NT-IIS                <00>  UNIQUE     Registered
EDUDOMAIN             <00>  GROUP      Registered
EDUDOMAIN             <1E>  GROUP      Registered
EDUDOMAIN             <1D>  UNIQUE     Registered
..__MSBROWSE__        <01>  GROUP      Registered
ADMINISTRATOR         <03>  UNIQUE     Registered
NT-IIS┐┐┐┐┐┐┐┐┐      <BF>  UNIQUE     Registered
```

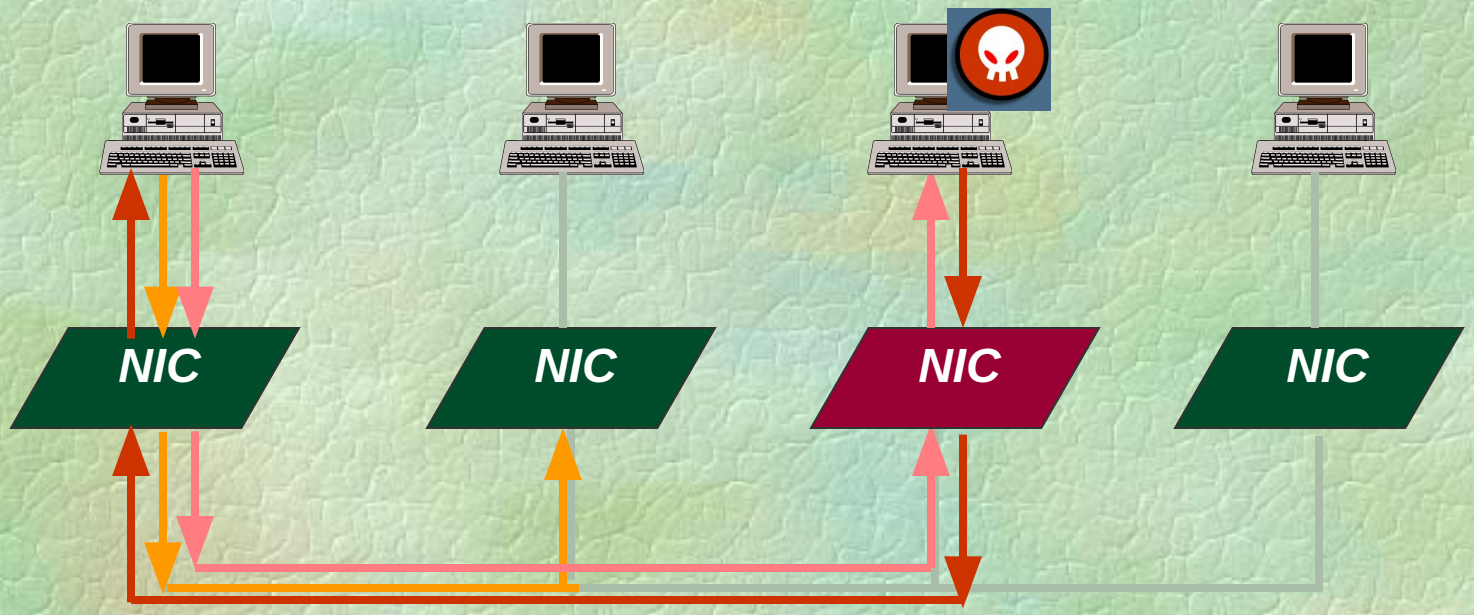
Технология обнаружения снифферов (UNIX)

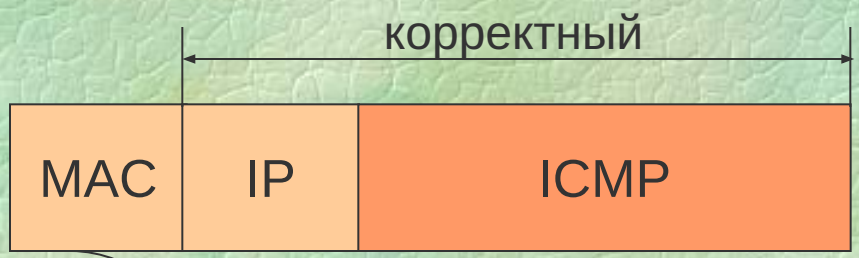




некорректный (несуществующий)
MAC-адрес получателя

Технология обнаружения снифферов (Windows)



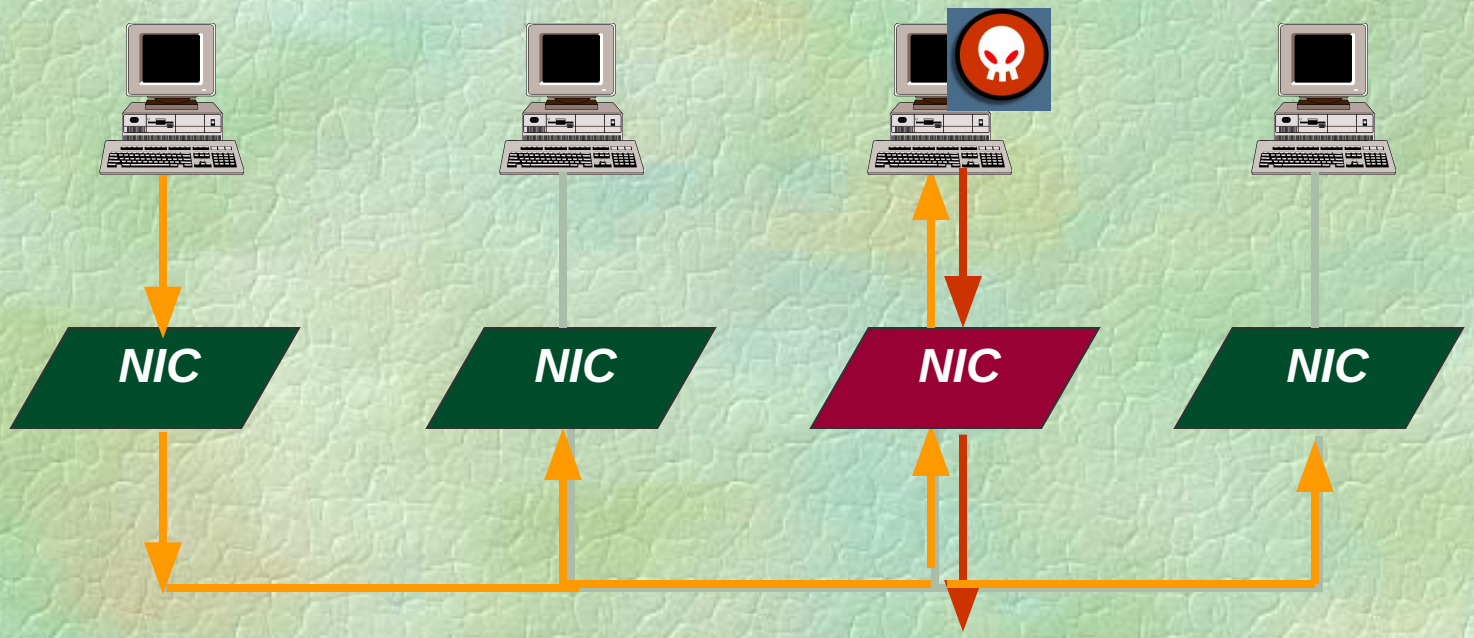


ff : ff : ff : ff : ff : ff

некорректный широковещательный MAC-адрес получателя

ff : 00 : 00 : 00 : 00 : 00

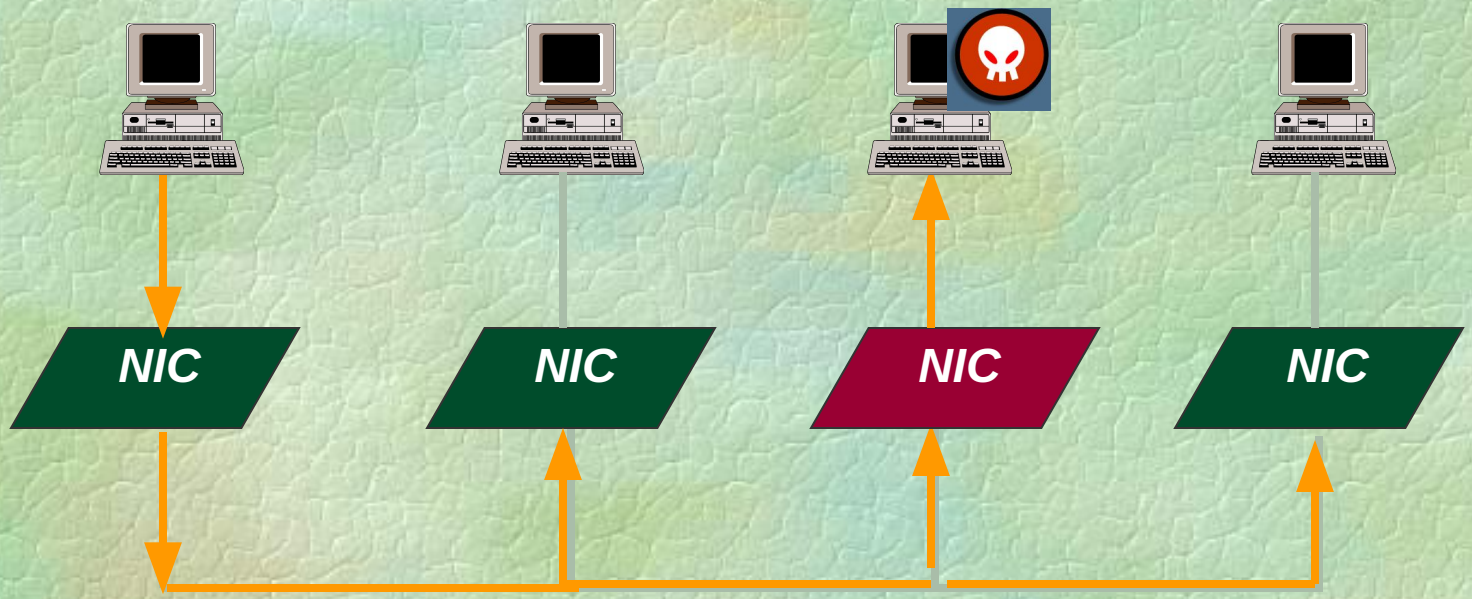
Технология обнаружения снифферов (DNS-тест)



Обратный DNS-запрос

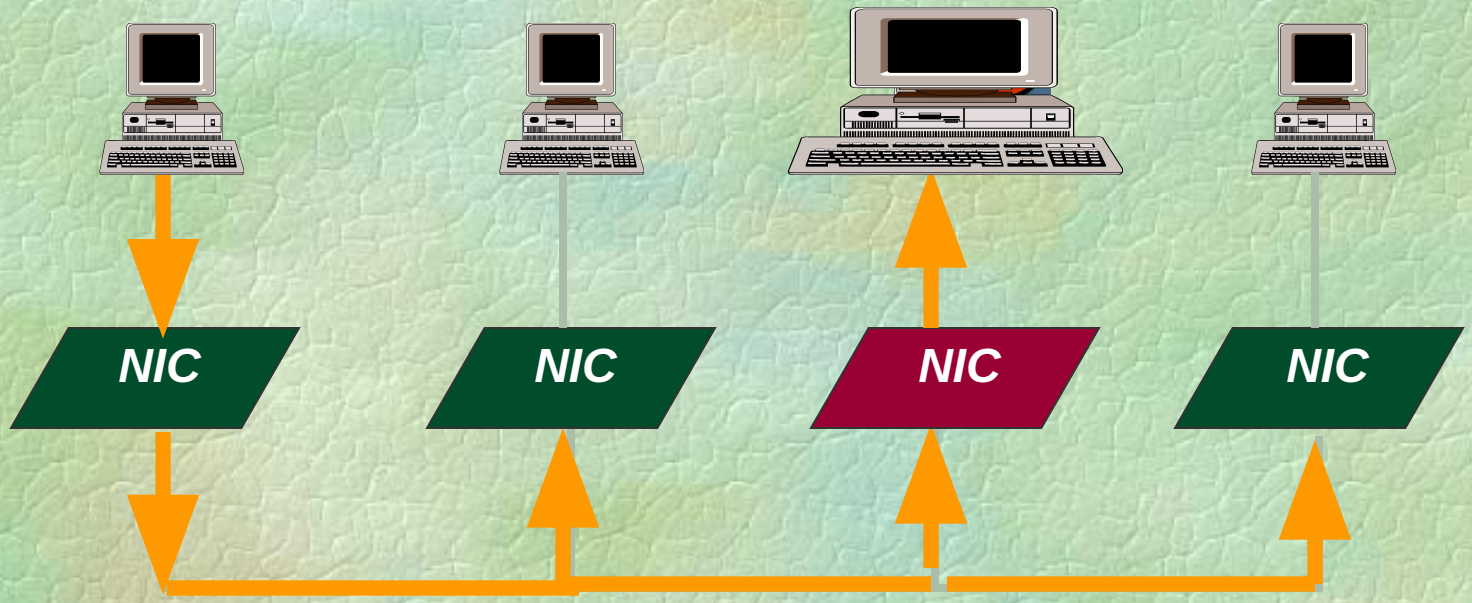
некорректный IP-адрес отправителя (получателя)

Технология обнаружения снифферов (анализ задержек)



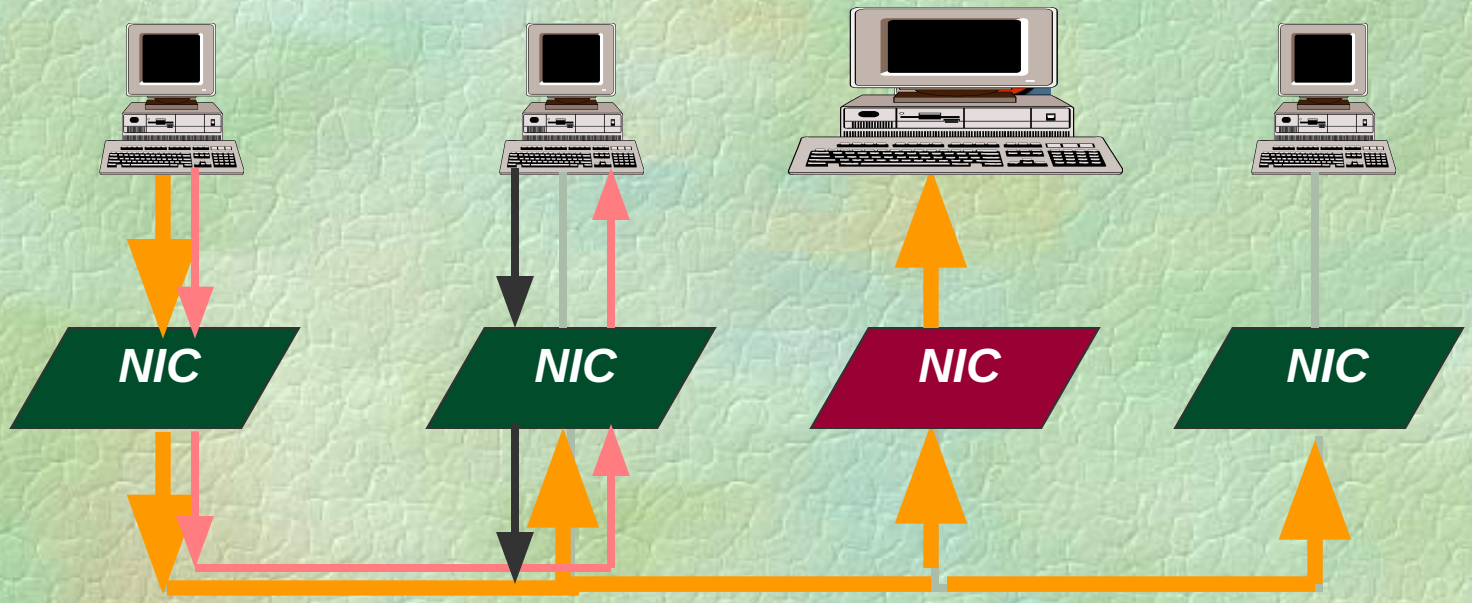
Обычный трафик

Технология обнаружения снифферов (анализ задержек)



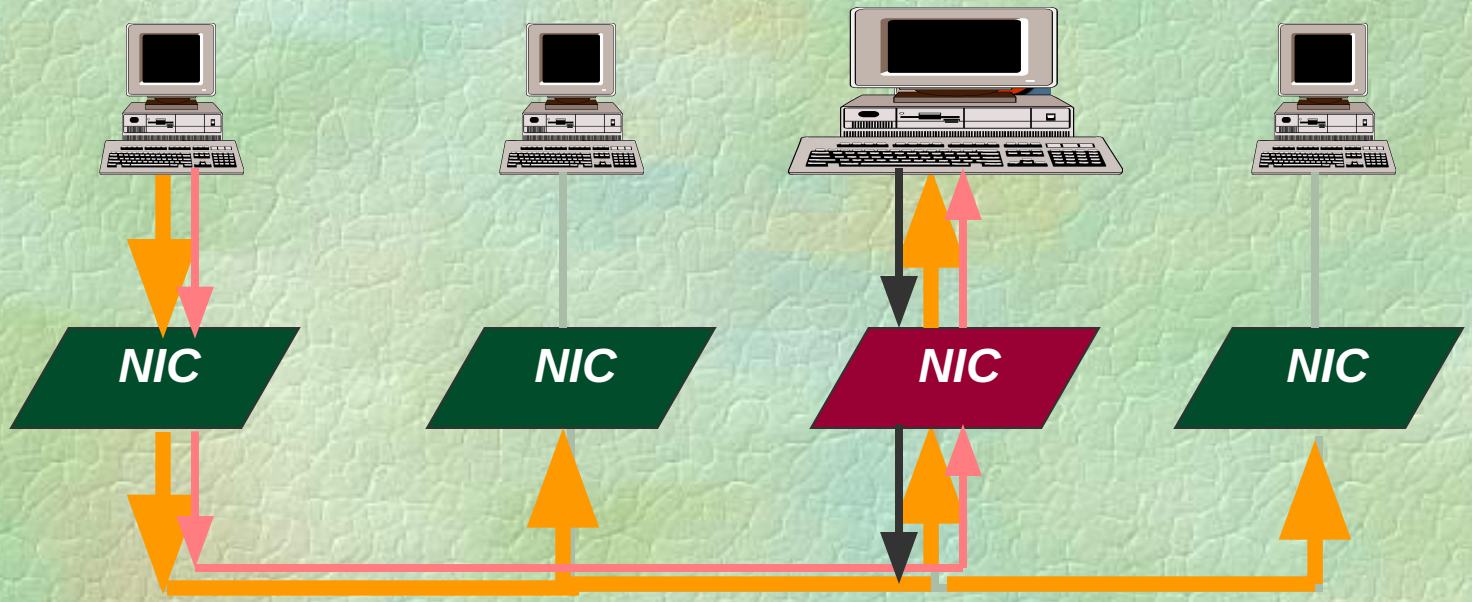
Увеличенный трафик

Технология обнаружения снифферов (анализ задержек)



Увеличенный трафик

Технология обнаружения снифферов (анализ задержек)



Увеличенный трафик

Протокол PPP

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

Link and Network Control Protocol
Full-Duplex Physical Link

RFC1331

Протокол PPP

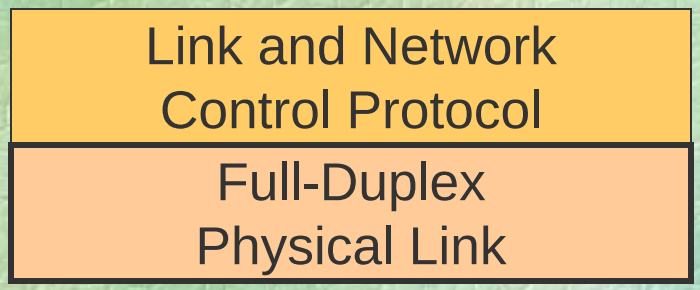
7	Уровень приложения
6	Уровень представления
5	Уровень соединения
4	Транспортный уровень
3	Сетевой уровень
2	Канальный уровень
1	Физический уровень

Link Control Protocol

Установление соединения

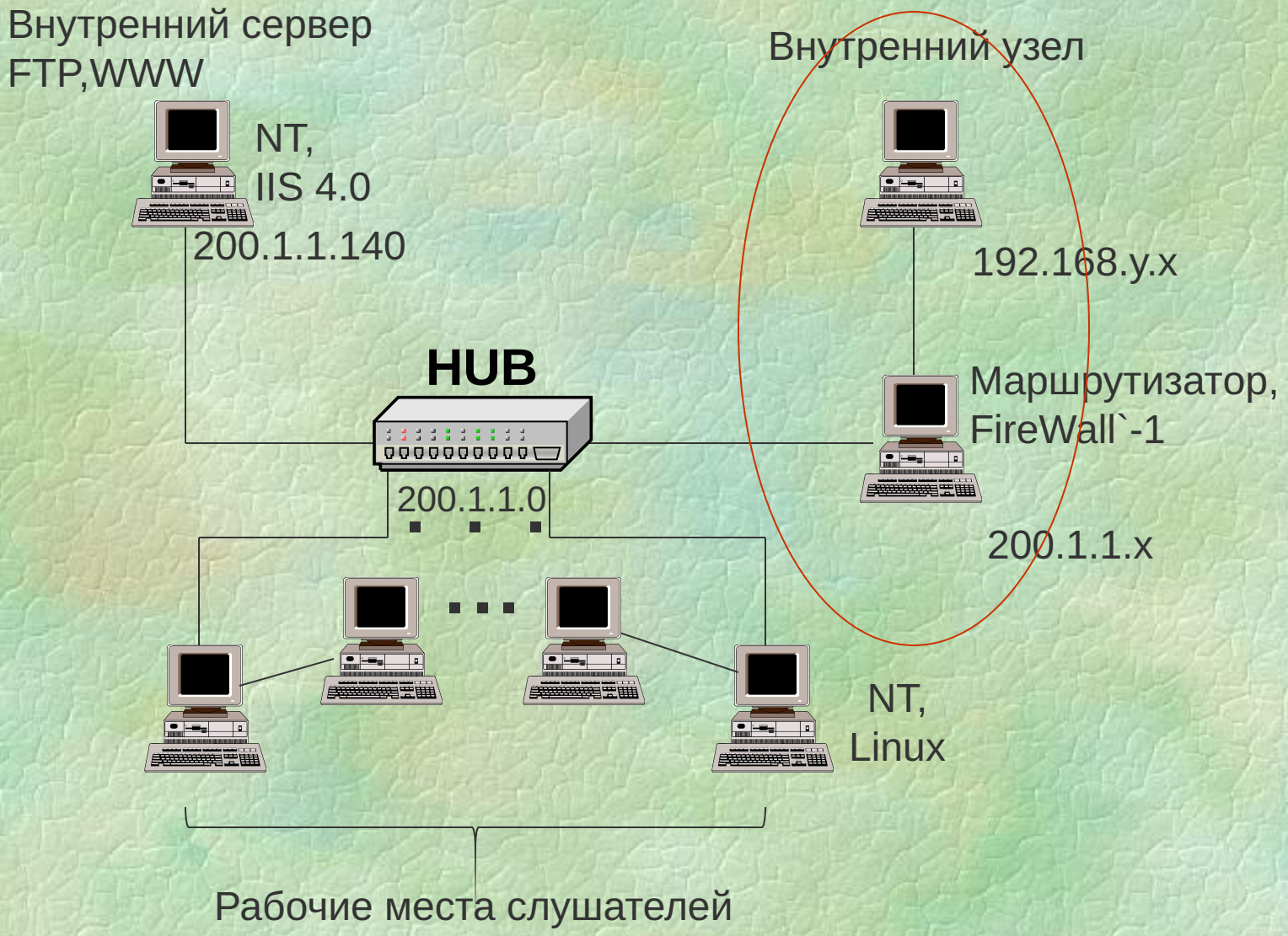
Network Control Protocol

Взаимодействие с IP, IPX

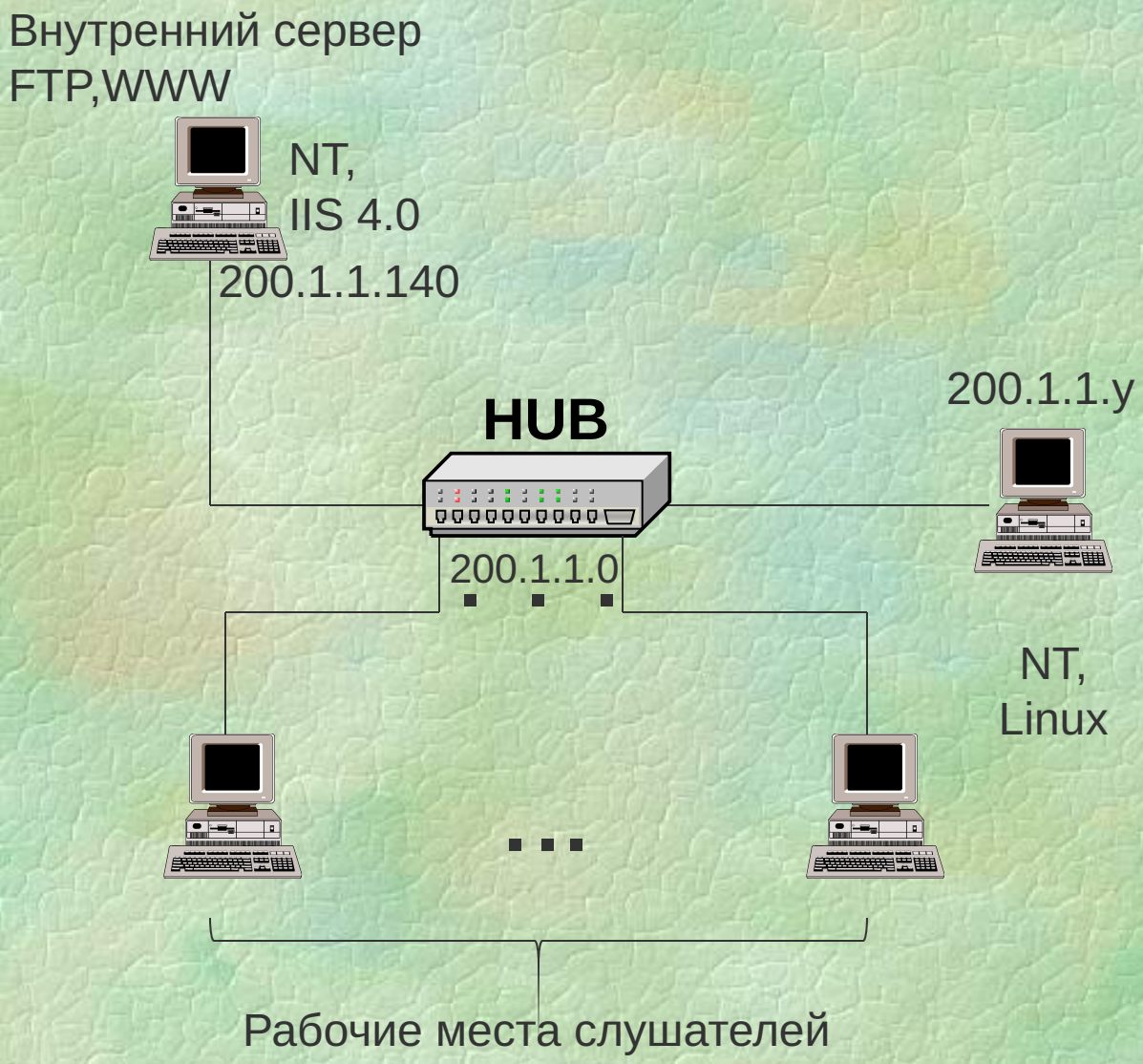


RFC1331

Конфигурация сети (попарная)



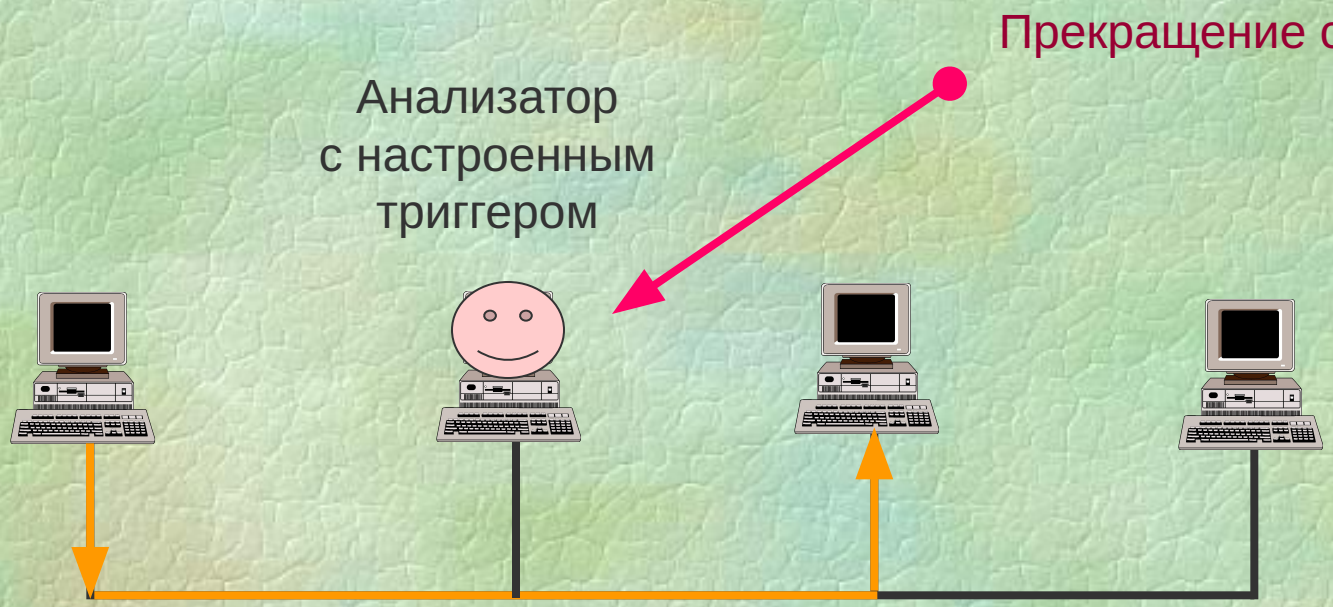
Конфигурация сети (обычная)



Практическая работа 2
Сетевые анализаторы

- Установка SnifferPro 1.5
- Основные приёмы работы с программой
- Фильтрация по различным критериям
- Работа с триггерами (пояснения далее)

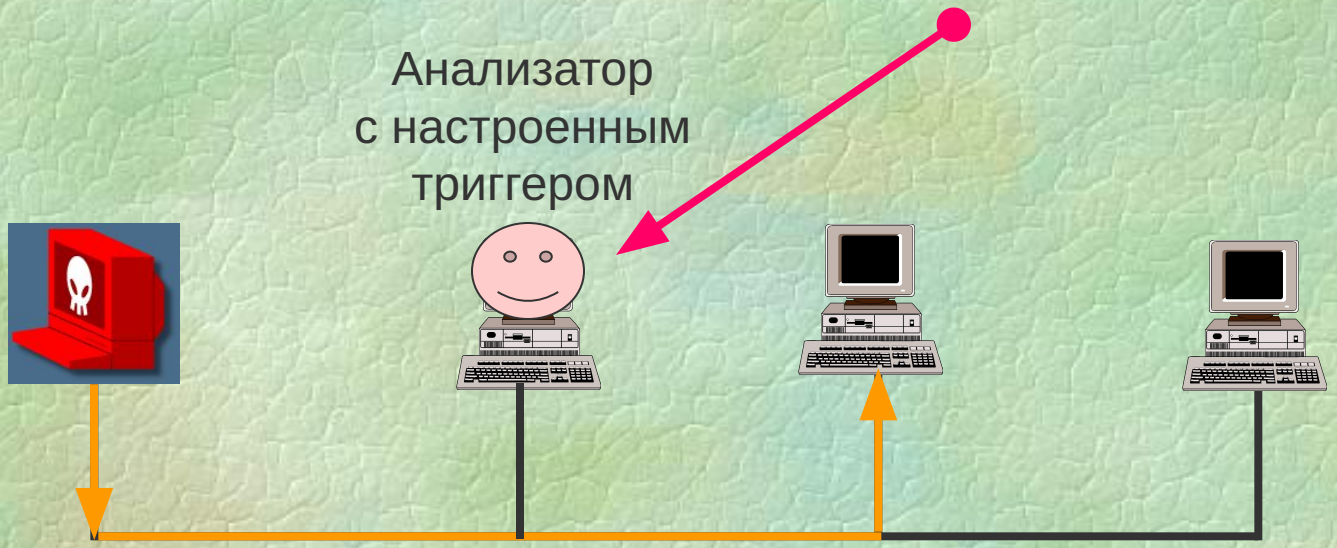
Триггеры для сетевых анализаторов



Пакет с определенным содержимым

Назначение триггеров

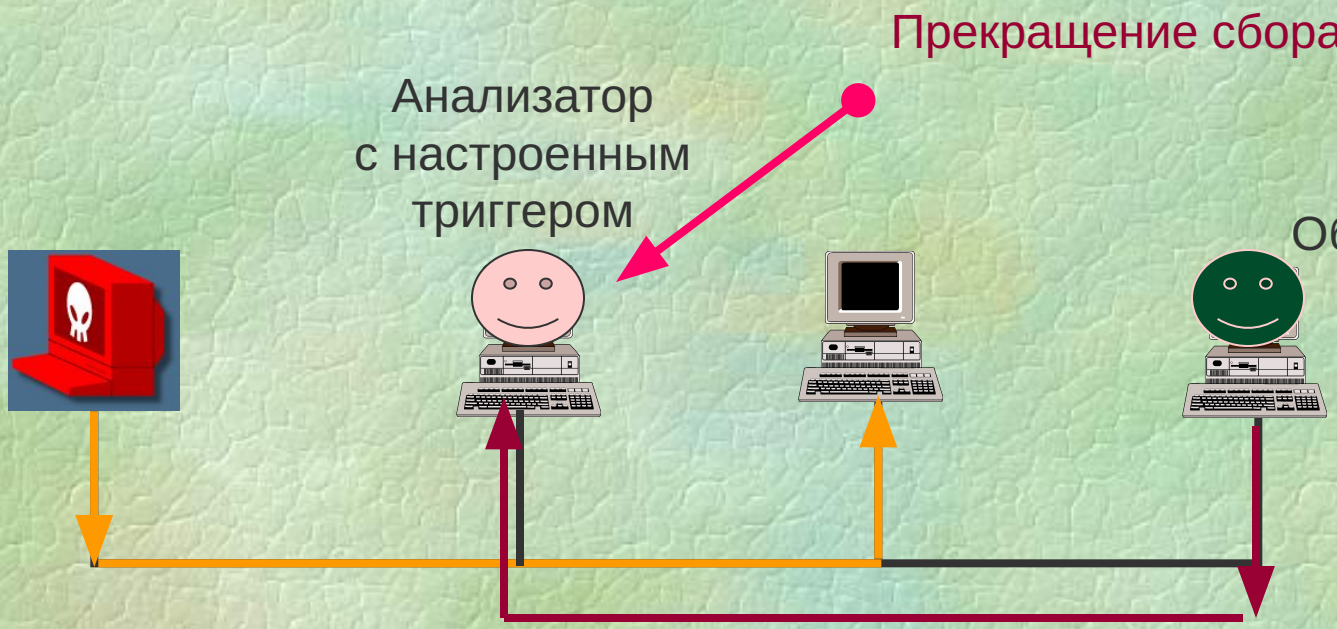
Атака WinNuke



OOB
Port=139

Обнаружение однопакетных атак

Назначение триггеров



Попытка атаки

Обнаружена атака

Пакет с определенным содержимым
(требуется настройка)

Взаимодействие с системами обнаружения атак