В общем случае кадры Ethernet могут быть четырёх различных форматов.[7] Далее перечислено назначение некоторых полей заголовка:

- Преамбула (8 байт) – сигнализирует о начале передачи.
- Адрес получателя (2-6 байт) – MAC-адрес получателя пакета.
- Адрес отправителя (2-6 байт) – MAC-адрес отправителя пакета.
- Длина (2 байта) – длина поля данных пакета.
- Контрольная сумма – используется для контроля целостности данных пакета.

## Адресация на канальном уровне (MAC-адрес)

Адресация на канальном уровне осуществляется при помощи аппаратных адресов (MAC-адресов, рис. 2.3). Существует три типа MAC-адресов:

- **Индивидуальный адрес (Individual)** – используется для идентификации отдельных узлов сети;
- **Широковещательный адрес (Broadcast)** – используется для обращения по всем узлам сетевого сегмента;
- **Групповой адрес (Multicast)** – используется для отправки сообщений логической группе узлов сети.

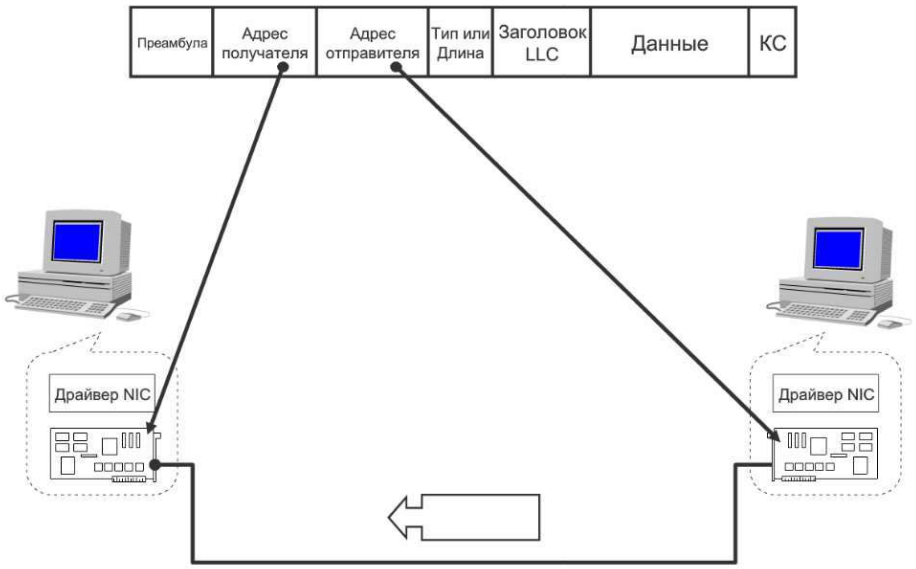



Рис. 2.3. Кадр Ethernet

На рисунке 2.4 показан формат индивидуального MAC-адреса. Два старших разряда всегда равны нулю. Далее идет идентификатор производителя (22 бита), присваиваемый комитетом IEEE производителям сетевого оборудования. Далее идет часть адреса, состоящая из 24 бит, определяемая самим производителем.

[7] Более подробное рассмотрение технологии Ethernet выходит за рамки данного курса. Этот и другие вопросы рассматриваются в курсе БТ05 «Основы TCP/IP».

| | | | |
|---|---|---|---|
| 0 | 0 | 22-бит идентификатора производителя | 24-бит адрес узла |

Рис. 2.4. MAC-адрес

## MAC-адрес и разграничение доступа

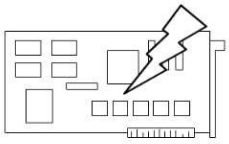
Довольно часто разграничение доступа основано на MAC-адресах. Например, оно может использоваться как дополнительный механизм защиты в беспроводных сетях, поскольку вероятность несанкционированного подключения к беспроводной сети выше, чем к сети, использующей кабели. Иногда аутентифицированные сессии учитываются по MAC-адресам клиентов. Возникает вопрос: насколько реальна подмена MAC-адреса (так называемый «MAC Address Spoofing»)?

MAC-адрес считывается через порт ввода-вывода сетевого адаптера в процессе загрузки операционной системы, помещается в память, а затем используется при выполнении операций с сетью.

Соответственно, изменить MAC-адрес узла можно следующими способами:

- На физическом уровне («перепрошивка» сетевого адаптера)
- В момент считывания в память ОС (например, в момент инициализации сетевого адаптера)
- На уровне ОС (например, путём редактирования реестра или конфигурационных файлов). Этот способ зависит от драйвера сетевого адаптера и от операционной системы

«Перепрошивка» адреса сетевого адаптера занимает считанные секунды, но требует дополнительного оборудования.



Изменение MAC-адреса в момент инициализации сетевого адаптера требует навыков работы с отладчиком. Для использования этого способа необходимо знать диапазон ввода-вывода сетевого адаптера и иметь какой-нибудь отладчик (например, SoftIce), загружающийся до операционной системы. При помощи отладчика можно отловить момент считывания MAC-адреса (например, при загрузке системы) и поменять его на требуемое значение (рис. 2.5).

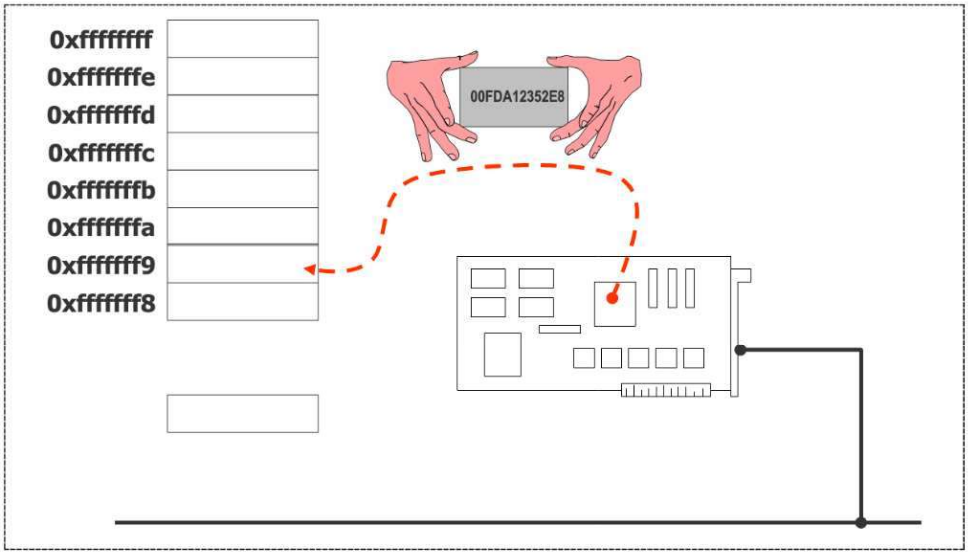



Рис. 2.5. Изменение MAC-адреса в момент загрузки ОС

И, наконец, третий способ изменения MAC-адреса – воспользоваться средствами ОС. Например, для ОС семейства Windows MAC-адрес можно задать в окне свойств сетевого адаптера. При отсутствии такой возможности можно воспользоваться редактором реестра. В этом случае потребуется создать несколько значимых элементов.

Для Windows 9x:

Ключ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net\0000

Значимые элементы

NetworkAddress="xx-xx-xx-xx-xx-xx" – Требуемый MAC-адрес
SelectedID="xx-xx-xx-xx-xx-xx" – Требуемый MAC-адрес

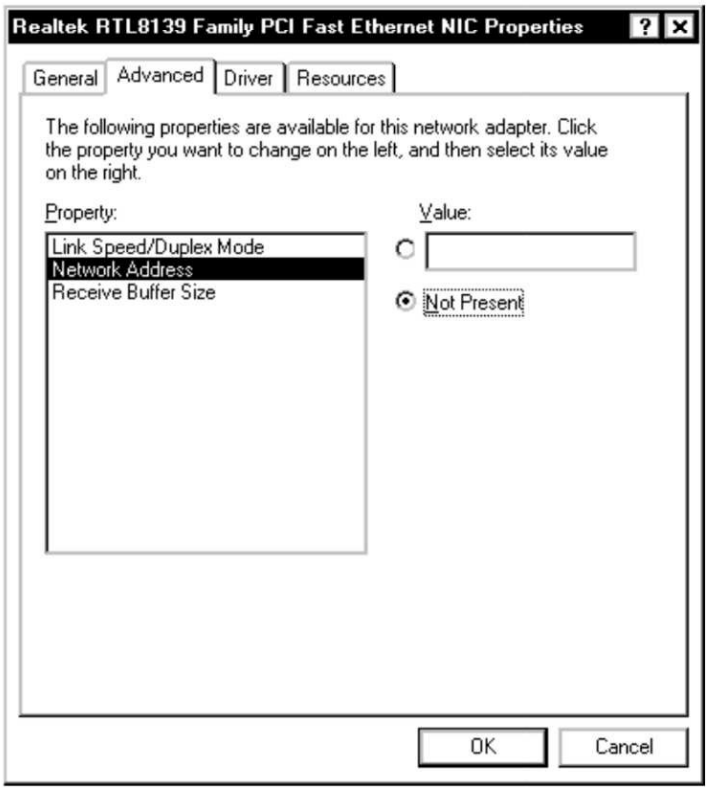
Для Windows NT/2000/XP/2003:

Ключ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\<сетевой адаптер>\номер

NetworkAddress="xx-xx-xx-xx-xx-xx"

Например, как на рисунке 2.6.

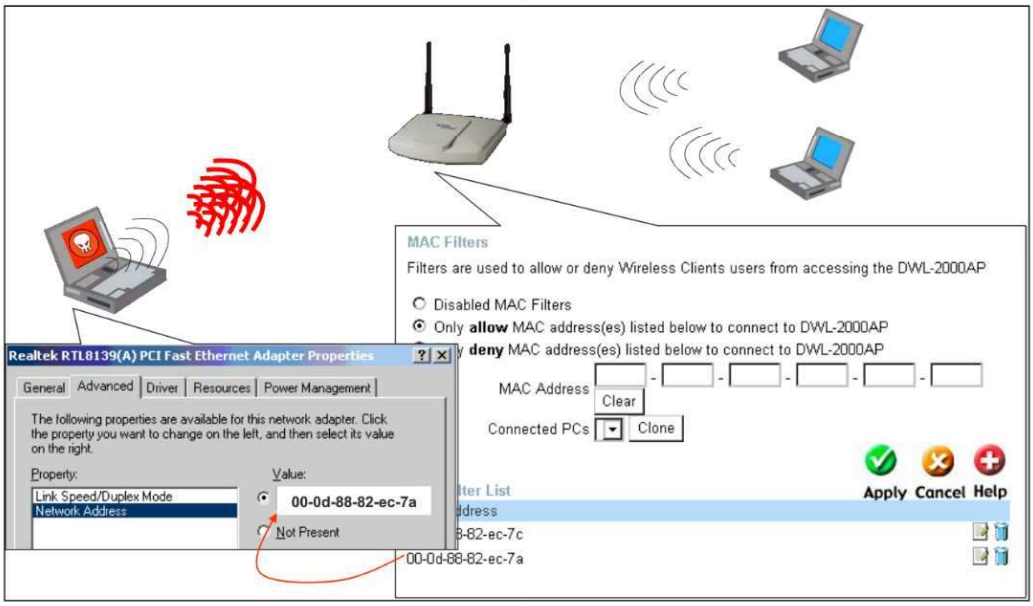
4. Нажать кнопку Update MAC
5. Перезапустить сетевой адаптер
6. Нажать кнопку Refresh
7. В списке вверху должен появиться новый MAC-адрес (дополнительно для проверки можно воспользоваться командой ipconfig /all).
8. Вернуть узлу исходный MAC-адрес, установив переключатель Value в положение Not Present.



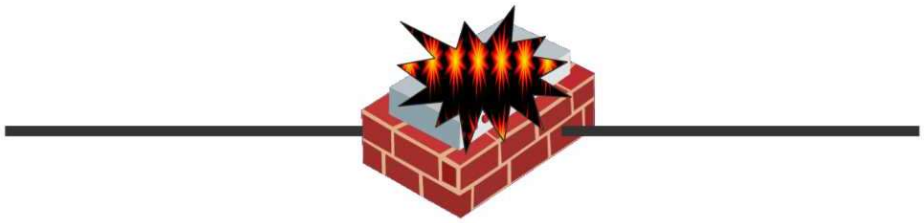
## Выводы (в каких случаях требуется изменение MAC-адреса)

Изменение MAC-адреса может быть полезным в следующих случаях:

- Тестирование систем на наличие уязвимостей аутентификации и авторизации на основе MAC-адресов (например, в беспроводных сетях).




- Резервирование узлов, при котором требуется точное совпадение имени, IP-адреса и MAC-адреса. Например, для того, чтобы не потребовалось обновление статических ARP-таблиц взаимодействующих 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
- Получение IP-адреса и других параметров по протоколу DHCP.

# Размер кадра Ethernet

## Ограничения на минимальный размер кадра Ethernet

Стандарт IEEE 802.3 (http://standards.ieee.org/getieee802/download/802.3-2005_section1.pdf) вводит ограничения на размер кадра Ethernet (п. 4.4.2): минимум 64 байта, максимум 1518 байт.

**4.4.2 Allowable implementations**

The following parameter values shall be used for their corresponding implementations:

| Parameters | Values | | |
|---|---|---|---|
| | 10 Mb/s<br>1BASE-5<br>100 Mb/s | 1 Gb/s | 10 Gb/s |
| slotTime | 512 bit times | 4096 bit times | not applicable |
| interFrameGap | 96 bits | 96 bits | 96 bits |
| attemptLimit | 16 | 16 | not applicable |
| backoffLimit | 10 | 10 | not applicable |
| jamSize | 32 bits | 32 bits | not applicable |
| maxUntaggedFrameSize | 1518 octets | 1518 octets | 1518 octets |
| minFrameSize | 512 bits (64 octets) | 512 bits (64 octets) | 512 bits (64 octets) |
| burstLimit | not applicable | 65 536 bits | not applicable |
| ifsStretchRatio | not applicable | not applicable | 104 bits |

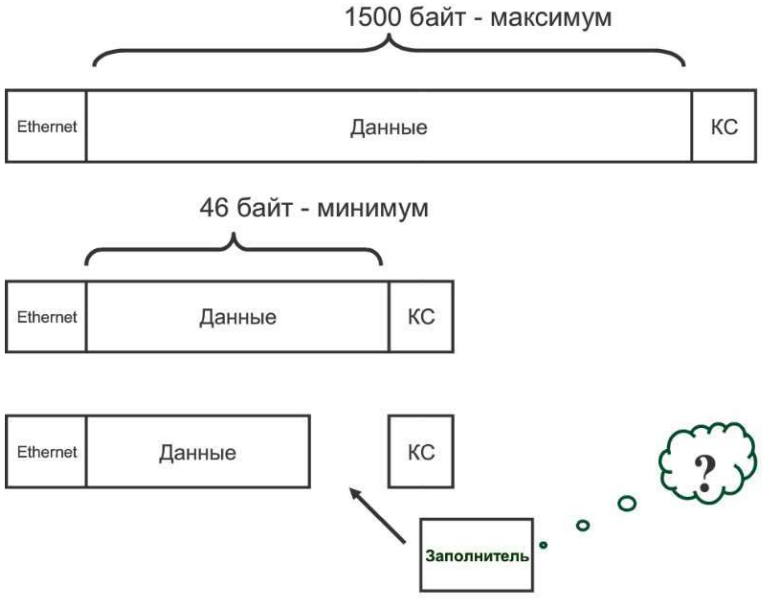
Как сказано в том же документе (п. 4.2.3.3), ограничение на минимальный размер фрейма связано с работой используемого в сетях Ethernet метода доступа к среде передачи CSMA/CD.

CSMA/CD IEEE Std 802.3-2005

**4.2.3.3 Minimum frame size**

The CSMA/CD Media Access mechanism requires that a minimum frame length of minFrameSize bits be transmitted. If frameSize is less than minFrameSize, then the CSMA/CD MAC sublayer shall append extra bits in units of octets (pad), after the end of the MAC client data field but prior to calculating and appending the FCS (if not provided by the MAC client). The number of extra bits shall be sufficient to ensure that the frame, from the DA field through the FCS field inclusive, is at least minFrameSize bits. If the FCS is (optionally) provided by the MAC client, the pad shall also be provided by the MAC client. The content of the pad is unspecified.

Таким образом, если размер фрейма меньше требуемого минимального значения (minFrameSize в документе), на подуровне MAC должен быть добавлен заполнитель. Заполнитель добавляется в конец поля данных, до расчёта контрольной суммы.




Операция дополнения кадра Ethernet может быть выполнена самим сетевым адаптером (это называется «автозаполнение») или его драйвером. При этом содержимое заполнителя не регламентируется. С операцией формирования заполнителя связана интересная уязвимость реализации некоторых драйверов, рассматриваемая далее.

### Описание уязвимости

Некоторые драйверы сетевых адаптеров не дополняют короткие пакеты нулевыми байтами, вместо этого в качестве заполнителя могут быть использованы фрагменты предыдущих пакетов или содержимое памяти ядра.

Индекс: CAN-2003-0001

Краткое описание: 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.

Ссылки:

ATSTAKE:A010603-1

URL:http://www.atstake.com/research/advisories/2003/a010603-1.txt

BUGTRAQ:20030110 More information regarding Etherleak

URL:http://marc.theaimsgroup.com/?l=bugtraq&m=104222046632243&w=2

VULNWATCH:20030110 More information regarding Etherleak

URL:http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0016.html

MISC:http://www.atstake.com/research/advisories/2003/atstake_etherleak_report.pdf

CERT-VN:VU#412115

URL:http://www.kb.cert.org/vuls/id/412115

Таким образом, содержимое заполнителя зависит от того, где расположен буфер, содержащий фрейм до его передачи. Вот возможные варианты:

- Dynamic kernel buffer (динамическая память ядра)

- Static device driver buffer (буфер драйвера сетевого адаптера)
- Hardware device transmit buffer (буфер сетевого адаптера)

В первом случае используется содержимое памяти ядра стека TCP/IP, поскольку часто фреймы строятся с участием стека TCP/IP.

Второй случай возникает тогда, когда драйвер перед передачей фрейма помещает его в свой собственный буфер.

В третьем случае фрейм может быть дополнен данными из буфера самого сетевого адаптера из-за того, что некоторые драйверы некорректно информируют сетевой адаптер о размере данных, помещаемых в его буфер. Поэтому в качестве заполнителя в этом случае выступает фрагмент предыдущего пакета.

### Почему это может быть опасно?

Данная уязвимость в большинстве случаев присуща драйверу сетевого адаптера, поэтому может проявляться на разных платформах. В принципе, она позволяет просматривать содержимое сетевых пакетов, аналогично сетевым анализаторам (рассматриваемым далее). Но, по сравнению с сетевыми анализаторами, использование этой уязвимости даёт нарушителю следующие преимущества:

- Возможность просмотра сетевого трафика в коммутируемых сетях
- Возможность целенаправленного сбора информации с сетевых объектов, таких как маршрутизаторы

Конечно, получение из собранных данных осмысленного текста может быть нетривиальной задачей, но в некоторых случаях можно получить например, содержимое HTTP-запросов или пароли, передаваемые по протоколам POP3, TELNET, FTP и т.д.

### Тестирование драйвера сетевого адаптера

Протестировать драйвер сетевого адаптера на наличие уязвимости можно следующим образом:

ping <тестируемый узел> -l 1 (для ОС Windows)


Команда отправляет на тестируемый узел ICMP «эхо-запрос» размером 1 байт. Размер IP-пакета при этом будет равен 29 байт, т. е. потребуется заполнитель. Таким образом, просмотрев пакет с ответом (сетевым анализатором) и проверив последние 17 байт

поля данных фрейма (чем они заполнены, нулями или нет), можно определить наличие рассматриваемой уязвимости.

### Драйверы из дистрибутива Windows Server 2003

По данным компании NGSSoftware (от 9 июня 2003) подобная уязвимость была обнаружена в некоторых драйверах сетевых адаптеров, поставляемых в составе Windows Server 2003. Результаты исследования можно найти по адресу: **http://www.nextgenss.com/advisories/etherleak-2003.txt**, а номер бюллетеня (Advisory number): #NISR09062003.

Уязвимость оказалась присуща следующим драйверам сетевых адаптеров:

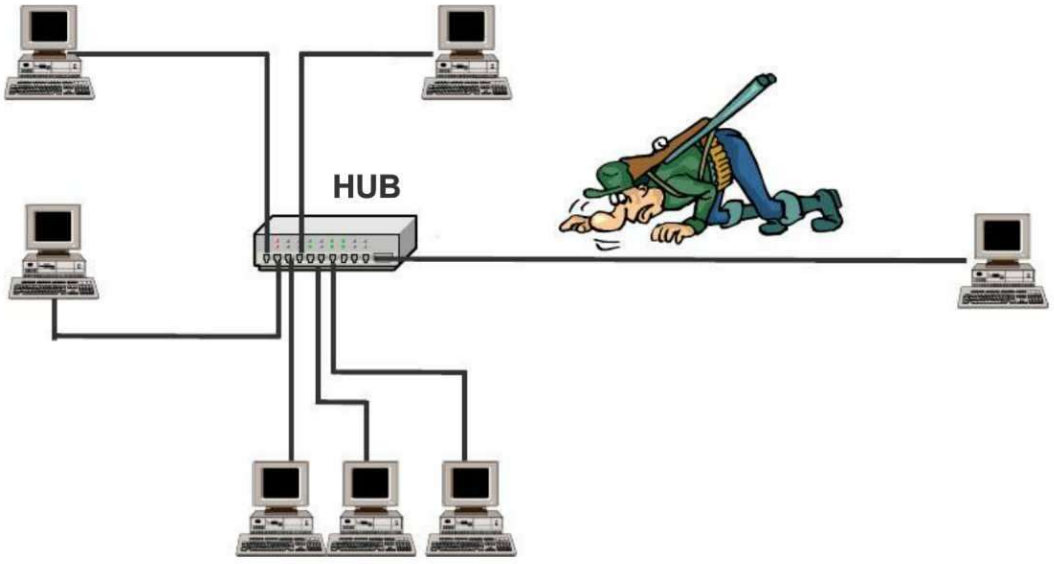
- VIA Rhine II Compatible (интегрированные с материнскими платами).
- AMD PCNet family (используются отдельными версиями VMware)

Указанные драйверы имеют цифровую подпись Microsoft Windows Publisher и входят в состав дистрибутива Windows Server 2003.

## Сетевые анализаторы ("снифферы")

### Что такое "сниффер"?

Сети Ethernet относятся к так называемым широковещательным сетям. Метод доступа, положенный в основу этой технологии, требует от узлов, подключённых к сети, непрерывного прослушивания всего сетевого трафика. Это означает, что узлы такой сети могут перехватывать информацию, адресованную своим соседям. Данная особенность технологии Ethernet делает возможным проведение атак, использующих механизм «пассивного прослушивания». Средства для проведения таких атак – это анализаторы протоколов или снифферы.

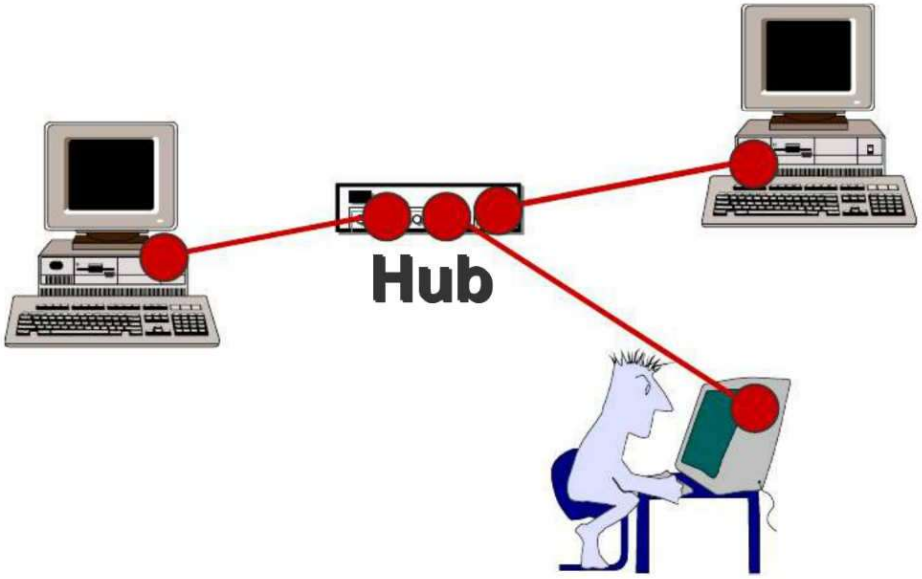



Термин "сниффер" («нюхач») впервые был использован компанией Network Associates в названии известного продукта "Sniffer (r) Network Analyzer". В самом общем смысле, слово "сниффер" обозначает устройство, подключенное к компьютерной сети и записывающее весь ее трафик подобно телефонным "жучкам", записывающим телефонные разговоры. Однако чаще всего "сниффером" называют программу,

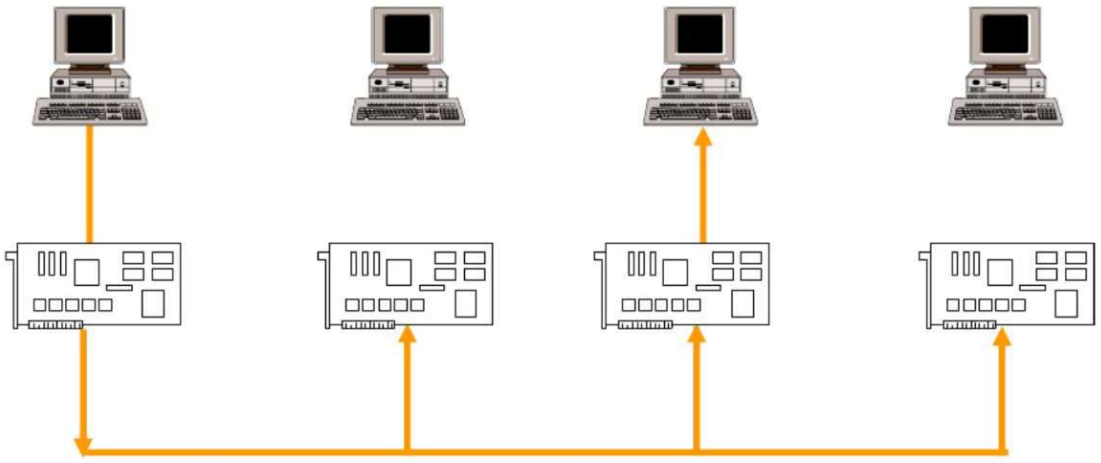
запущенную на подключенном к сети узле и просматривающую весь трафик сетевого сегмента.

### Как работает “сниффер”?

Работа “сниффера” использует основной принцип технологии Ethernet – общую среду передачи. Это означает, что любое устройство, подключенное к сетевому сегменту, может слышать и принимать все сообщения, в том числе предназначенные не ему.




Сетевые адаптеры Ethernet могут работать в двух режимах: селективном (non-promiscuous) и неселективном (promiscuous). В первом случае, принимаются только сообщения, предназначенные данному узлу. Выбор осуществляется на основе MAC-адреса фрейма.



Во втором случае фильтрация не осуществляется, и узел принимает все фреймы, передаваемые по сегменту.

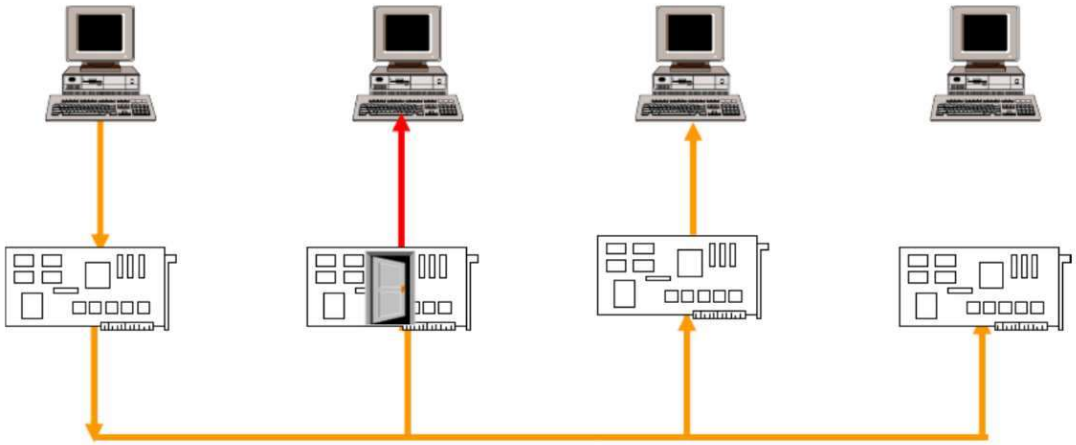
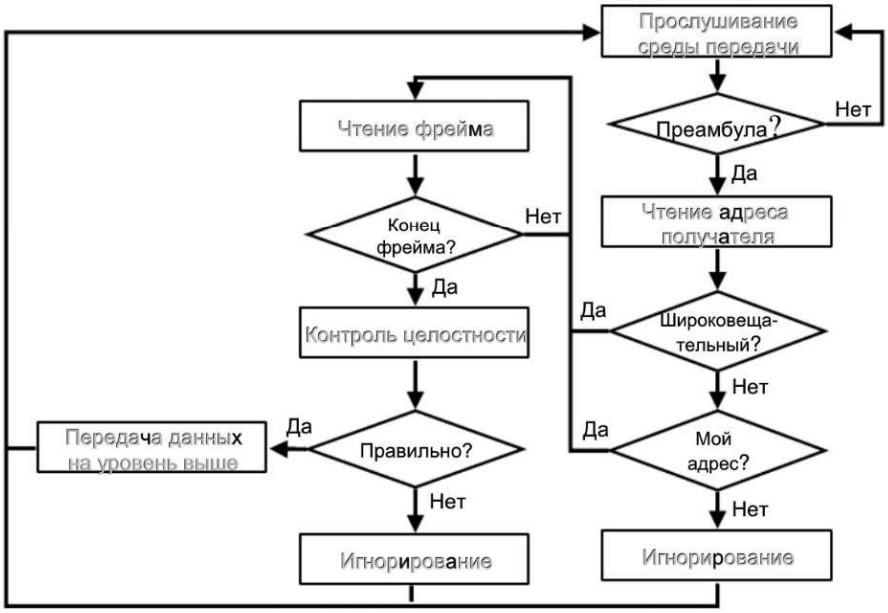
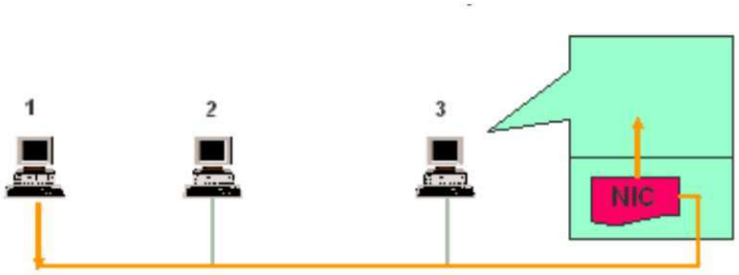


Схема алгоритма работы сетевого адаптера при приёме данных (селективный режим) приведена на следующем рисунке.




Таким образом, в неселективном режиме сетевые адаптеры принимают все фреймы, в том числе и не предназначенные данному узлу, единственное проверяемое условие – целостность фрейма.




- Пакет прошёл проверку целостности

Специализированные программы, переводящие сетевой адаптер в неселективный режим и собирающие весь трафик сети для последующего анализа, называются анализаторами протоколов или «снифферами». Собранный трафик сегмента может быть отображен на экране, записан в файл и т.п. Так как компьютеры обмениваются по сети двоичной информацией, в обязанности “сниффера” обычно входит так называемый структурный анализ протоколов (включающий разбиение пакета на заголовки и данные) и вывод информации в удобном (читаемом) виде.

Анализатор протоколов – программный продукт “двойного” применения. Он может быть использован специалистами и администраторами сетей для анализа происходящих в сети процессов и диагностики неисправностей. С другой стороны, снифферы используются злоумышленниками для проведения атак (механизм атаки - “пассивное прослушивание”). Кроме того, тот же принцип пассивного прослушивания трафика лежит в основе работы средств обнаружения сетевых атак.

Итак, анализаторы протоколов позволяют злоумышленнику просматривать весь трафик сетевого сегмента. Возможен ли перехват информации в случае нахождения злоумышленника в другом сегменте? С помощью анализатора протоколов это осуществить невозможно, однако для этого используются другие методы, позволяющие перенаправить трафик из другого сегмента на узел нарушителя и реализующие атаки типа «создание ложного объекта-посредника» на сетевом и транспортном уровнях модели OSI.

В сети Internet можно найти множество анализаторов протоколов для различных операционных систем. Далее перечислены некоторые из них:

- CommView
- Network Monitor
- Ethereal (Wireshark)
- tcpdump

Все они, обладая похожим функционалом, работают по изложенным выше принципам.

## Меры защиты от “снифферов”

Меры защиты от снифферов следуют из принципа их работы и цели атак:

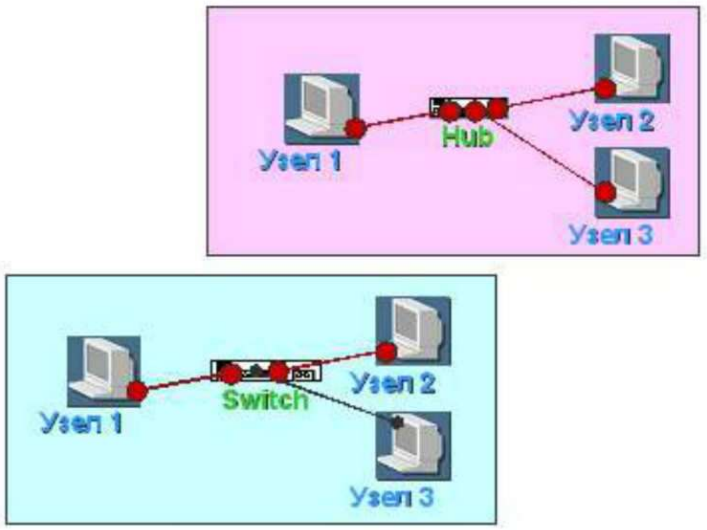
- **Шифрование информации**. Так как целью прослушивания обычно является перехват критичной (конфиденциальной) информации, то эта мера защиты сделает невозможным последующий анализ перехваченных данных.

- **Построение сетей на основе интеллектуальных коммутаторов (switches)**. Это аппаратное решение проблемы, сводящее к минимуму “общую среду передачи”. При использовании коммутаторов можно обеспечить режим, когда каждая рабочая станция будет работать в своем отдельном сегменте.
- **Использование сетевых адаптеров, не поддерживающих неселективный режим**. Некоторые из сетевых адаптеров не поддерживают неселективный режим на аппаратном уровне, другие снабжаются драйвером, не допускающим работу в неселективном режиме.
- **Обнаружение несанкционированно используемых на компьютерах анализаторов протоколов**. Как было указано выше, обнаружить сниффер достаточно сложно. Однако существуют программные средства, разработанные для этой цели – **антисниффферы**. В качестве примера можно привести программный продукт Antisniff компании Lopht, пробная версия которого доступна по адресу: **www.lopht.com**.

Далее некоторые из перечисленных мер защиты рассматриваются более подробно.

### Применение коммутаторов

Очевидно, что в сети, построенной на базе коммутаторов, нарушитель не имеет возможности перехватить пакеты, если они адресованы не ему, так как пакет направляется не во все порты (как на концентраторе), а лишь в тот, к которому подключен получатель.




Но в этом случае способы прослушивания могут быть основаны на:

- Уязвимостях коммутаторов.
- Использовании механизма ARP-Spoofing (более подробно рассматривается в разделе, посвящённом протоколу ARP).

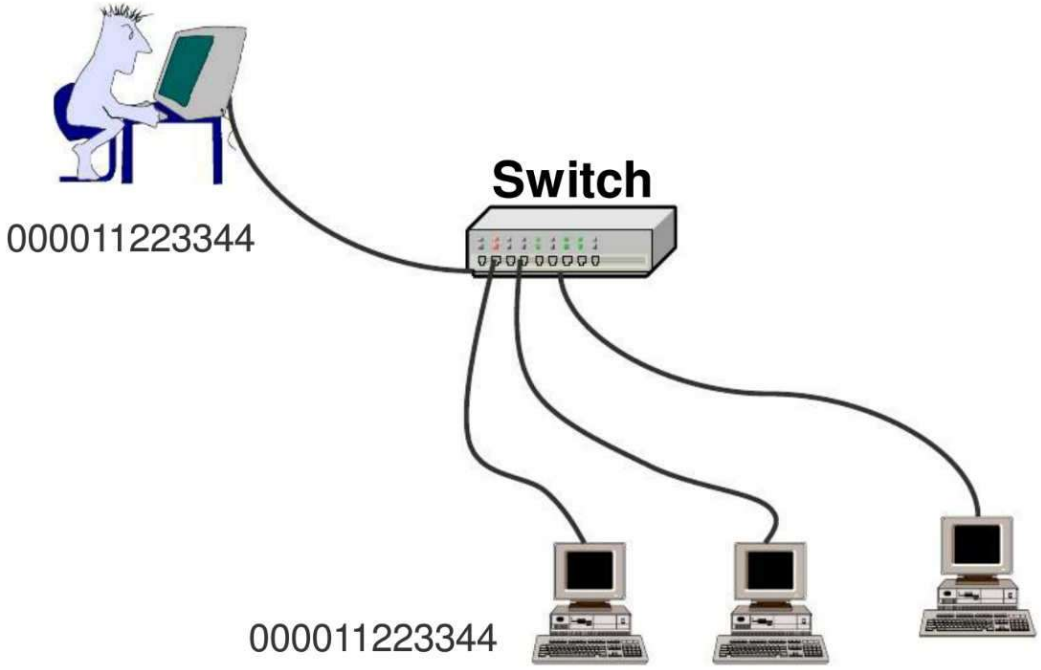
Что касается уязвимостей коммутаторов, то в качестве примеров можно привести следующие способы:

- Генерация большого количества сетевых пакетов с различными MAC-адресами источника. Это приводит к переполнению таблицы коммутации, в которой

хранятся соответствия между MAC-адресами и портами на коммутаторе. Как следствие, коммутатор переводится в режим концентратора.

- Очистка таблицы коммутации (например, путём использования каких-либо уязвимостей) и перевод коммутатора в режим «обучения». При этом на некоторое время коммутатор превращается в концентратор. Подробнее на эту тему можно прочитать в [16].

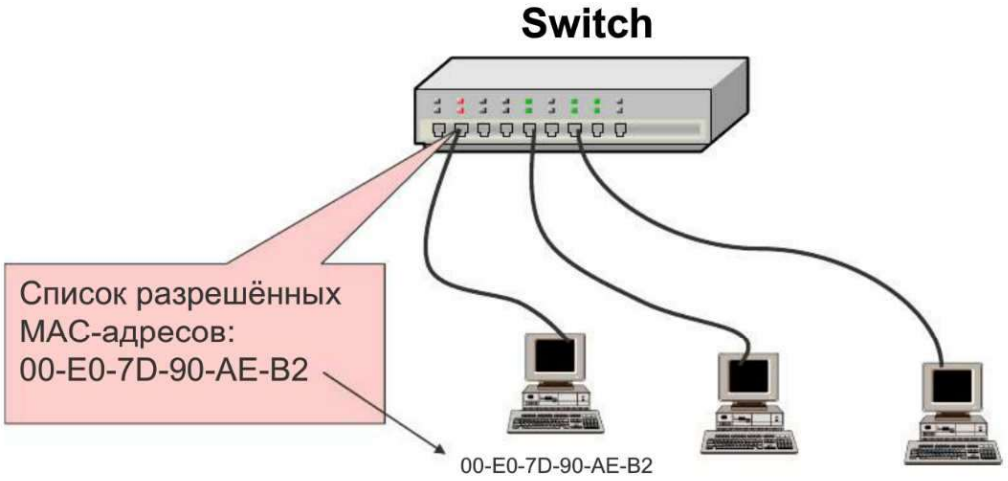
Отдельного рассмотрения заслуживает ситуация назначения двух одинаковых MAC-адресов узлам, подключенным к одному и тому же коммутатору.




Возникает вопрос, какому из узлов будет передан пакет, у которого в качестве адреса получателя задан указанный на рисунке MAC-адрес.

### Port Security

Механизм «**Port Security**» служит для защиты от несанкционированного подключения к порту коммутатора. Реализуется это путём формирования списка MAC-адресов, разрешённых для данного порта. Если MAC-адрес отправителя в заголовке фрейма не принадлежит указанному списку, пакет отбрасывается. Этот список должен быть сформирован администратором и «привязан» к порту. Если этот список не задан, некоторые коммутаторы при включении функции «**Port Security**» заносят в него 1-й встретившийся MAC-адрес и впоследствии разрешают только его.




Этот механизм позволяет в случае обнаружения атаки идентифицировать её источник с точностью до порта на коммутаторе.

Разумеется, механизм «**Port Security**» не может контролировать подлинность MAC-адреса, т. е. не защищает от подмены MAC-адреса. Эта функция контролирует лишь значение MAC-адреса отправителя в заголовке фрейма.

### Обнаружение снифферов

Так как сниффер по определению имеет «пассивную» природу, обнаружить его достаточно сложно.

Тем не менее, обнаружить факт прослушивания трафика в отдельных случаях всё-таки можно. Тесты, позволяющие это сделать, можно поделить на следующие группы:

- По косвенным признакам (основанным на особенностях реализации)
- Тесты, учитывающие особенности реализации стека TCP/IP в ОС
- DNS-тесты
- Анализ задержек
- Использование протокола ARP (наиболее эффективный метод)[8]

Далее некоторые из перечисленных методов рассматриваются более подробно.

Иногда присутствие сниффера можно обнаружить по каким-либо косвенным признакам, свойственным конкретному снифферу. В частности, Network Monitor (из состава Windows NT Server 4.0) версий 1.x при запуске регистрирует свое NetBIOS - имя, которое можно увидеть командой nbtstat. В следующем примере имя, зарегистрированное программой Network Monitor, в списке идёт последним (последний байт имени - <BF>).

[8] Более подробно рассматривается в разделе, посвящённом протоколу ARP

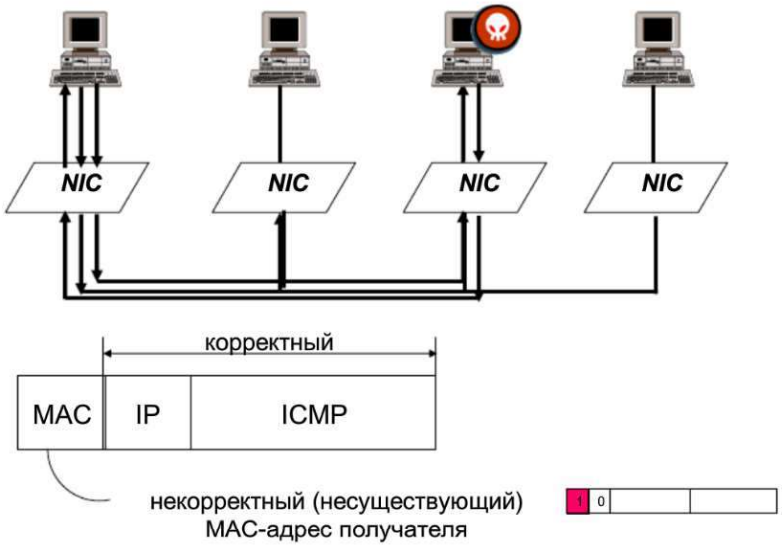
```
E:\>nbtstat -n

        NetBIOS Local Name Table

  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

E:\>
```

Следующая группа тестов основана на особенностях обработки различными ОС специальным образом построенных пакетов. Например, если отправить в сеть пакет с несуществующим MAC-адресом получателя (например, программа **AntiSniff** использует адрес `66:66:66:66:66:66`), но с корректно построенным IP-заголовком (например, ICMP-запрос), то некоторые версии UNIX при работе адаптера в неселективном режиме ответят на такой пакет.




DNS-тест основывается на том факте, что очень часто снифферы пытаются определить имена узлов на основе собранной информации (например, при помощи обратных DNS-запросов). Программа **AntiSniff** переводит сетевой адаптер в неселективный режим и посылает в сеть пакеты, содержащие несуществующие адреса. Если каким-либо узлом, подключенным к сегменту, будет послан обратный DNS-запрос по какому-либо адресу, делается предположение о работе сетевого адаптера узла в неселективном режиме.