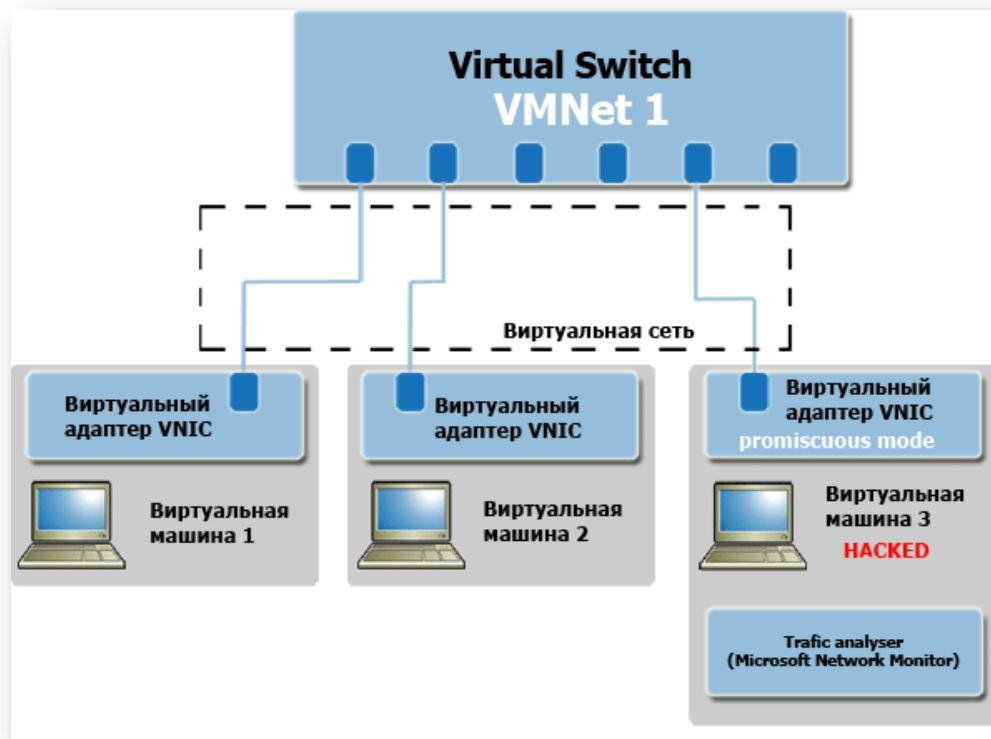


# АНАЛИЗАТОРЫ СЕТЕВЫХ ПАКЕТОВ



# СНИФФЕРЫ

- Анализаторы сетевых пакетов, или sniffеры, первоначально были разработаны как средство решения сетевых проблем.
- Они умеют перехватывать, интерпретировать и сохранять для последующего анализа пакеты, передаваемые по сети.

The screenshot displays the Jitbit Network Sniffer application. The interface includes a control panel with 'Start', 'Stop', and 'Clear' buttons, a 'Network Interface' dropdown set to '192.168.37.32', and 'Hex' and 'Text' packet view options. Below this is a table of captured packets:

Time	Src IP	Dest IP	Proto	Length	Src Port	Dest Port
16.27.33.298	192.168.37.222	192.168.37.32	TCP	308	4564	2754
16.27.33.455	192.168.37.32	192.168.37.222	TCP	40	2754	4564
16.27.33.455	192.168.37.222	192.168.37.32	TCP	660	4564	2754
16.27.33.658	192.168.37.32	192.168.37.222	TCP	40	2754	4564
16.27.34.330	192.168.37.222	192.168.37.32	TCP	1500	4564	2754
16.27.34.330	192.168.37.222	192.168.37.32	TCP	1500	4564	2754
16.27.34.330	192.168.37.32	192.168.37.222	TCP	40	2754	4564
16.27.34.330	192.168.37.222	192.168.37.32	TCP	1500	4564	2754
16.27.34.330	192.168.37.222	192.168.37.32	TCP	1500	4564	2754
16.27.34.330	192.168.37.32	192.168.37.222	TCP	40	2754	4564

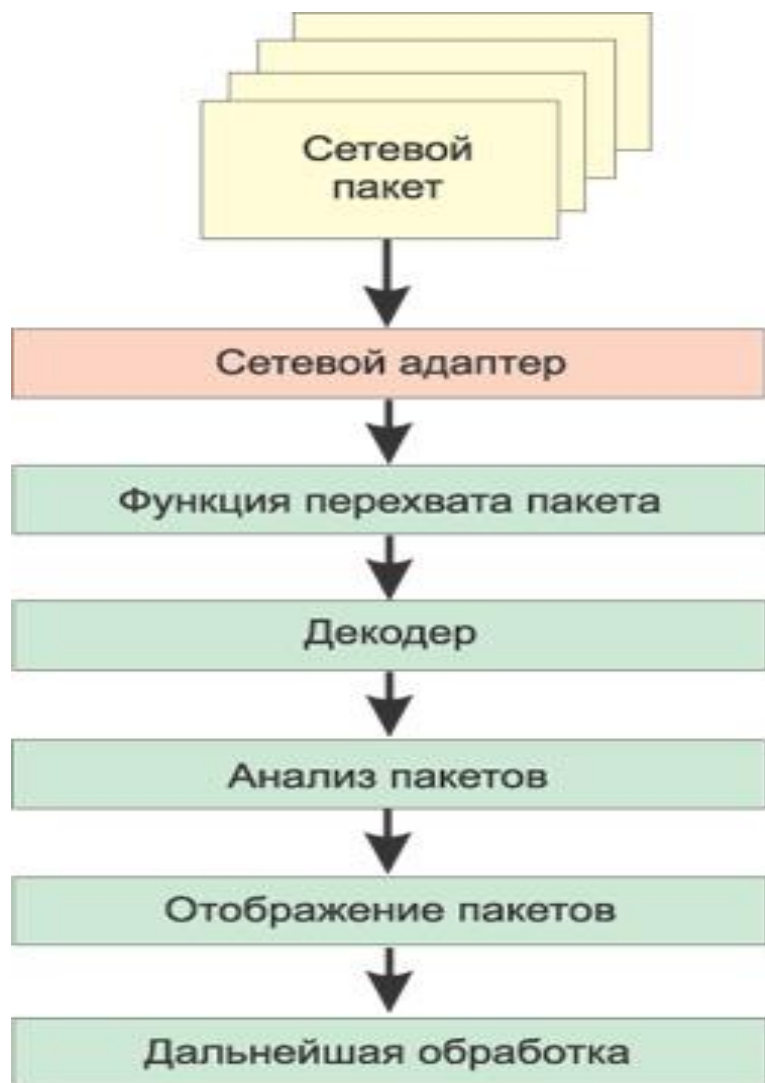
The detailed view shows the hex and ASCII representation of a packet header:

```
4500 0028 E899 4000 8006 45E7 C0A8 2520 E...{i**@ T. EsAE%
C0A8 25DE 0AC2 11D4 23AF D3A6 9CF9 188D AE%Ю. В. ФН| ъш. К
5010 FC87 1D8B 0000 P. ь±. < . .
```

The IP Header details are as follows:

- Header length: 5
- Version: 4
- Service type: 0
- Total length: 40
- ID: 59545
- Offset: 16384
- TTL: 128
- Protocol: 6
- Check Sum: 17895
- Src IP: 192.168.37.32
- Dest IP: 192.168.37.222

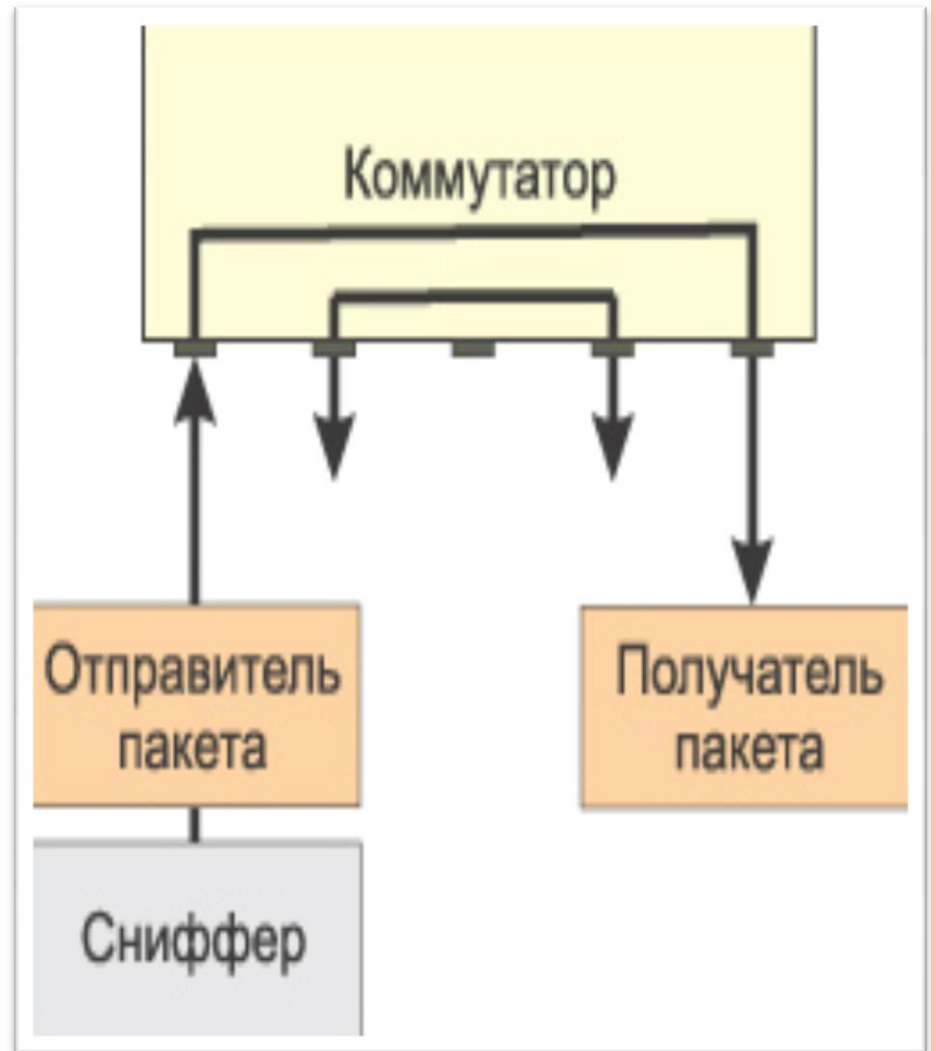
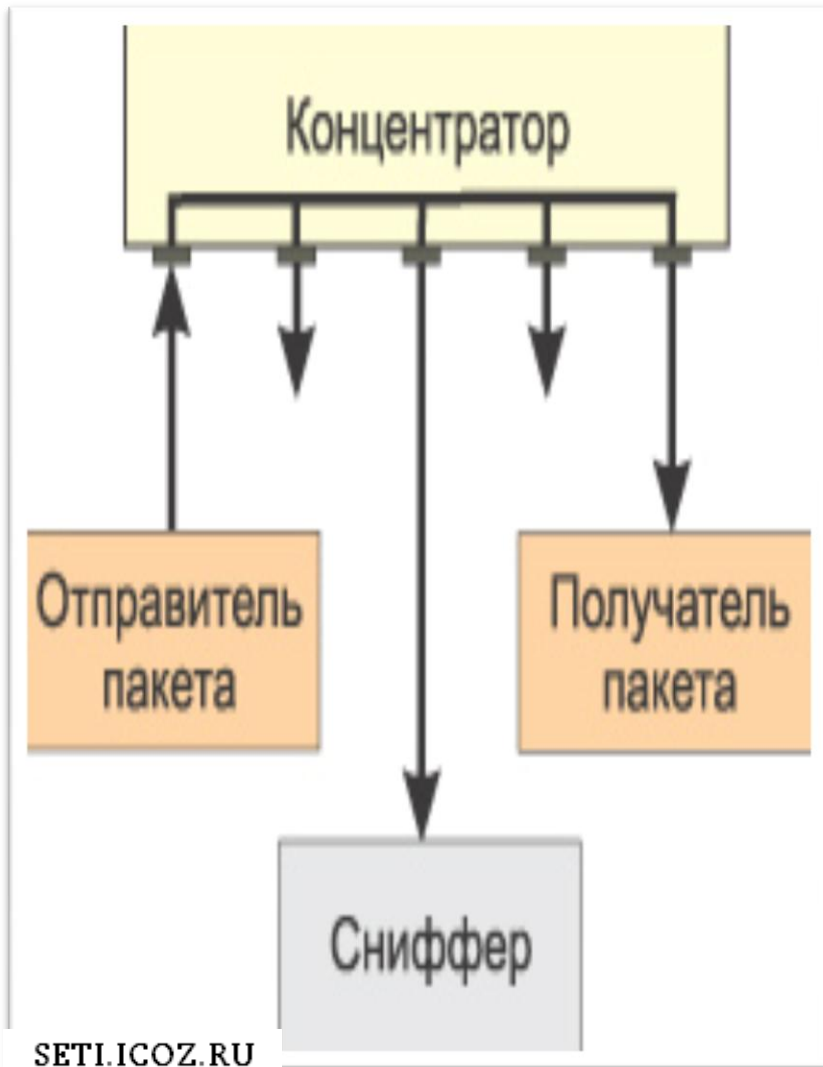
# ПРИНЦИПЫ РАБОТЫ ПАКЕТНЫХ СНИФФЕРОВ



**Сниффер** — это программа, которая работает на уровне сетевого адаптера NIC (Network Interface Card) (канальный уровень) и скрытым образом перехватывает весь трафик.

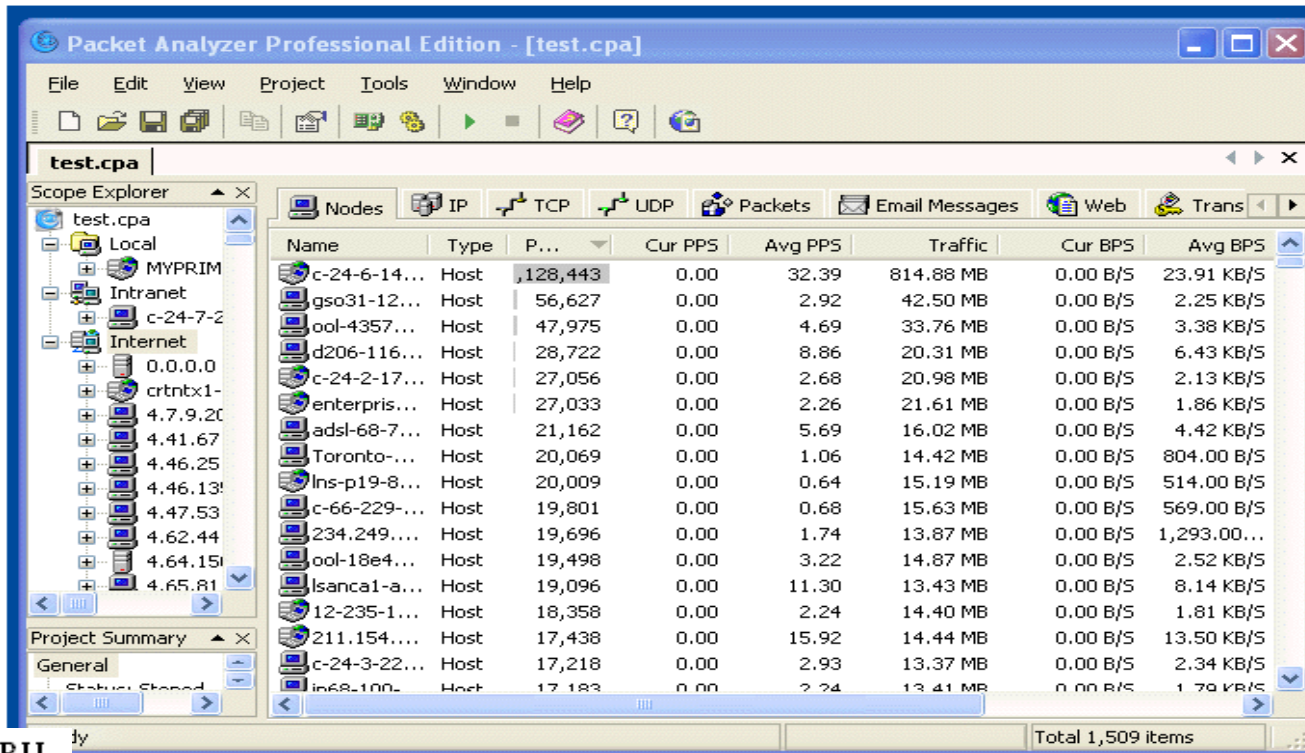


# ИСПОЛЬЗОВАНИЯ СНИФФЕРОВ



# МЕТОДЫ ПЕРЕХВАТА СЕТЕВОГО ТРАФИКА

- Прослушивание сети с помощью программ сетевых анализаторов, является первым, самым простым способом перехвата данных.



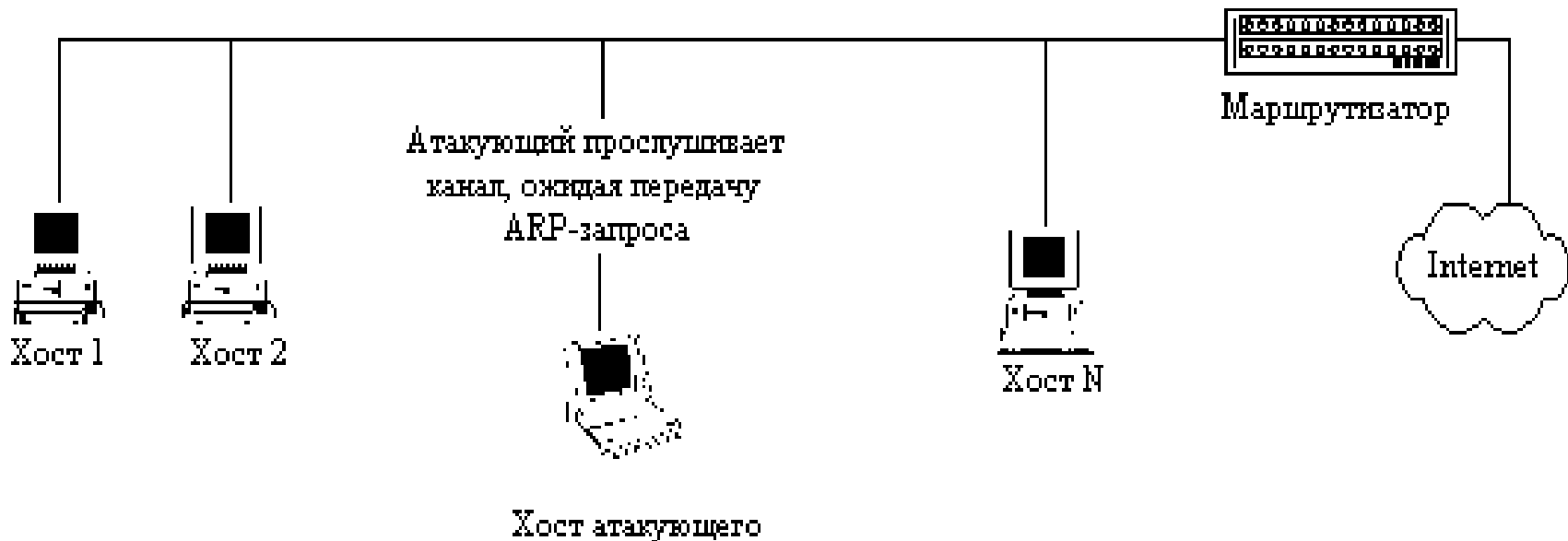
The screenshot shows the Packet Analyzer Professional Edition interface. The main window displays a table of network traffic data. The table has columns for Name, Type, P... (Packets), Cur PPS (Current Packets Per Second), Avg PPS (Average Packets Per Second), Traffic, Cur BPS (Current Bytes Per Second), and Avg BPS (Average Bytes Per Second). The table lists various hosts and their traffic statistics.

Name	Type	P...	Cur PPS	Avg PPS	Traffic	Cur BPS	Avg BPS
c-24-6-14...	Host	128,443	0.00	32.39	814.88 MB	0.00 B/S	23.91 KB/S
gso31-12...	Host	56,627	0.00	2.92	42.50 MB	0.00 B/S	2.25 KB/S
ool-4357...	Host	47,975	0.00	4.69	33.76 MB	0.00 B/S	3.38 KB/S
d206-116...	Host	28,722	0.00	8.86	20.31 MB	0.00 B/S	6.43 KB/S
c-24-2-17...	Host	27,056	0.00	2.68	20.98 MB	0.00 B/S	2.13 KB/S
enterpris...	Host	27,033	0.00	2.26	21.61 MB	0.00 B/S	1.86 KB/S
adsl-68-7...	Host	21,162	0.00	5.69	16.02 MB	0.00 B/S	4.42 KB/S
Toronto-...	Host	20,069	0.00	1.06	14.42 MB	0.00 B/S	804.00 B/S
Ins-p19-8...	Host	20,009	0.00	0.64	15.19 MB	0.00 B/S	514.00 B/S
c-66-229...	Host	19,801	0.00	0.68	15.63 MB	0.00 B/S	569.00 B/S
234.249...	Host	19,696	0.00	1.74	13.87 MB	0.00 B/S	1,293.00...
ool-18e4...	Host	19,498	0.00	3.22	14.87 MB	0.00 B/S	2.52 KB/S
Isanca1-a...	Host	19,096	0.00	11.30	13.43 MB	0.00 B/S	8.14 KB/S
12-235-1...	Host	18,358	0.00	2.24	14.40 MB	0.00 B/S	1.81 KB/S
211.154...	Host	17,438	0.00	15.92	14.44 MB	0.00 B/S	13.50 KB/S
c-24-3-22...	Host	17,218	0.00	2.93	13.37 MB	0.00 B/S	2.34 KB/S
in68-100...	Host	17,183	0.00	2.24	13.41 MB	0.00 B/S	1.78 KB/S

- Для защиты от прослушивания сети применяются специальные программы, например, **AntiSniff** , которые способны выявлять в сети компьютеры, занятые прослушиванием сетевого трафика.
- Программы-антисниферы для решения своих задач используют особый признак наличия в сети прослушивающих устройств - сетевая плата компьютера-снифера должна находиться в специальном режиме прослушивания.
- Находясь в режиме прослушивания, сетевые компьютеры особенным образом реагируют на IP-дейтаграммы, посылаемые в адрес тестируемого хоста.

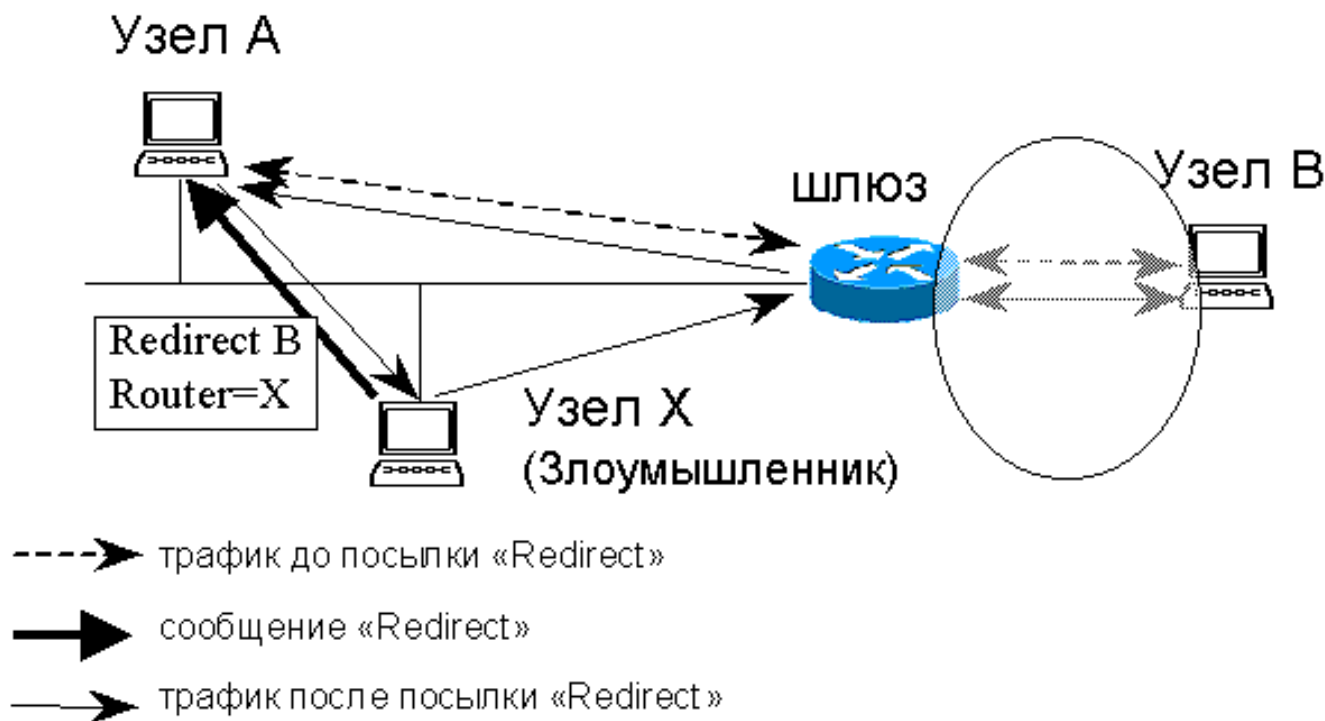
# ЛОЖНЫЕ ЗАПРОСЫ ARP

- Чтобы перехватить и замкнуть на себя процесс сетевого взаимодействия между двумя хостами А и В злоумышленник может подменить IP-адреса взаимодействующих хостов своим IP-адресом, направив хостам А и В фальсифицированные сообщения ARP (Address Resolution Protocol - Протокол разрешения адресов).



## МАРШРУТИЗАЦИЯ

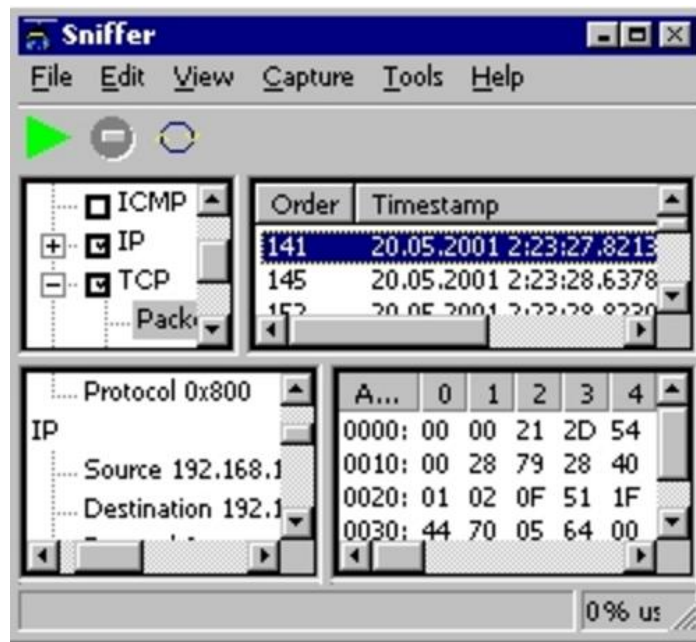
- Чтобы перехватить сетевой трафик, злоумышленник может подменить реальный IP-адрес сетевого маршрутизатора своим IP-адресом, выполнив это, например, с помощью фальсифицированных ICMP-сообщений Redirect.





# ПЕРЕХВАТ TCP-СОЕДИНЕНИЯ

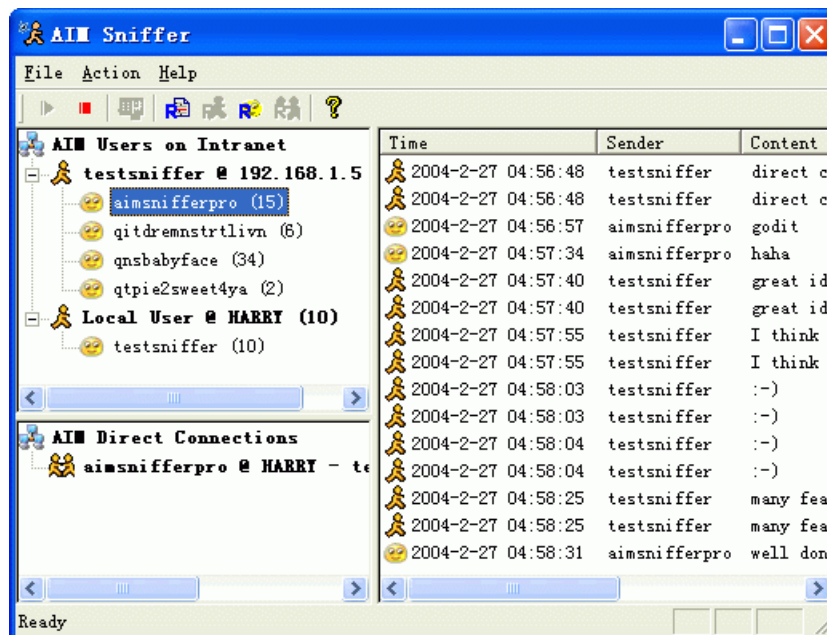
- Захват TCP-соединения (TCP hijacking) –это когда злоумышленник путем генерации и отсылки на атакуемый хост TCP-пакетов прерывает текущий сеанс связи с хостом. Далее, пользуясь возможностями протокола TCP по восстановлению прерванного TCP-соединения, хакер перехватывает прерванный сеанс связи и продолжает его вместо отключенного клиента.



# ОБЗОР ПРОГРАММНЫХ ПАКЕТНЫХ СНИФФЕРОВ

Категории программ-снифферов :

- снифферы, поддерживающие запуск из командной строки,
- снифферы, имеющие графический интерфейс.
- снифферы, которые объединяют в себе обе эти ВОЗМОЖНОСТИ



- Практически все пакетные снифферы позволяют производить анализ декодированных пакетов (именно поэтому пакетные снифферы также называют пакетными анализаторами, или протокольными анализаторами).
- Сниффер распределяет перехваченные пакеты по уровням и протоколам. Некоторые анализаторы пакетов способны распознавать протокол и отображать перехваченную информацию.



- Существуют программные снифферы, к которым в качестве плагинов или встроенных модулей прилагаются программные аналитические модули, позволяющие создавать отчеты с полезной аналитической информацией о перехваченном трафике.
- Другая характерная черта большинства программных анализаторов пакетов — возможность настройки фильтров до и после захвата трафика. Фильтры выделяют из общего трафика определенные пакеты по заданному критерию, что позволяет при анализе трафика избавиться от лишней информации.



## ПЕРЕЧЕНЬ УЧЕБНЫХ ИЗДАНИЙ, ИНТЕРНЕТ-РЕСУРСОВ, ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ ИСПОЛЬЗОВАННОЙ ПРИ СОЗДАНИИ ПРЕЗЕНТАЦИИ

- Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
- Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство [электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2009. – 944 с., ил.
- Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс]. — Режим доступа: URL: <http://www.ccc.ru/> (дата обращения: 03.09.12).
- Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]. — Режим доступа: URL: <http://www.intuit.ru/> (дата обращения: 03.09.12).
- Журнал CHIP [Электронный ресурс]. — Режим доступа: URL: <http://www.ichip.ru/> (дата обращения: 03.09.12).
- Журнал "Computer Bild" [Электронный ресурс]. — Режим доступа: URL: <http://www.computerbild.ru> (дата обращения: 03.09.12).