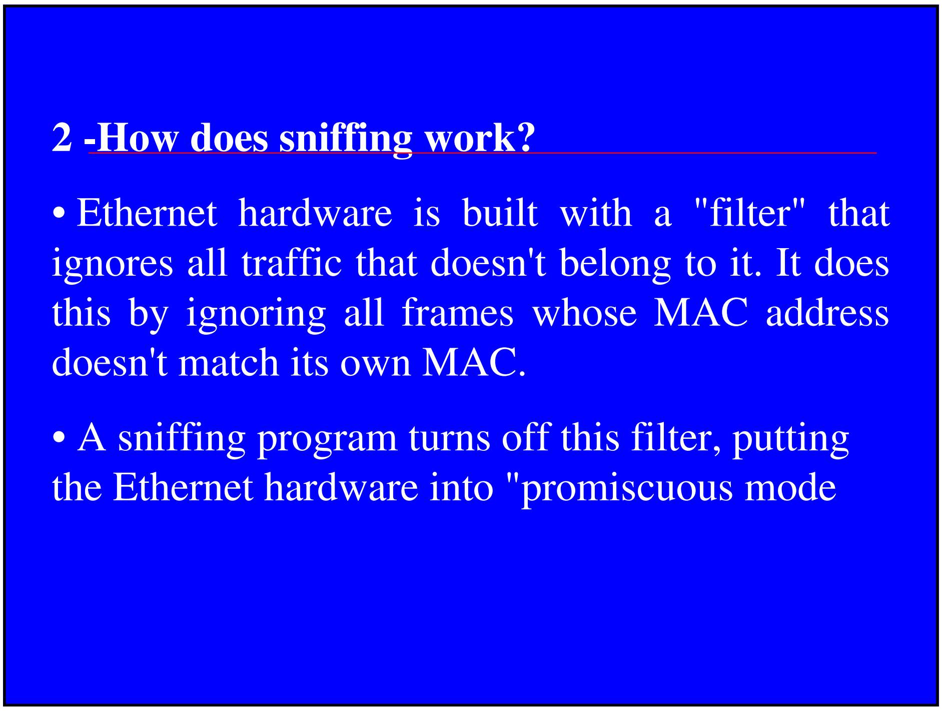
Sniffers

Definition :

- **packet sniffer** is a wire-tap devices that plugs into computer networks and eavesdrops on the network traffic, then decodes this traffic in a process called " Protocol Analysis " .

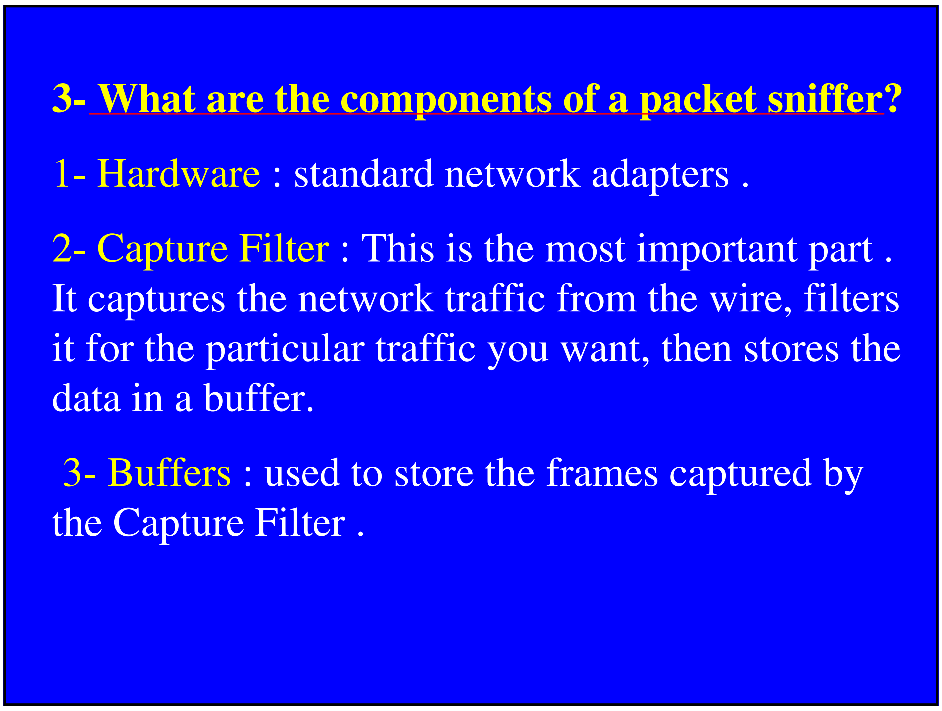
1- What is it used for?

- Detection of clear-text passwords and usernames from the network.
- Conversion of data to human readable format so that people can read the traffic.
- Performance analysis to discover network bottlenecks.
- Network intrusion detection in order to discover hackers



2 -How does sniffing work?

- Ethernet hardware is built with a "filter" that ignores all traffic that doesn't belong to it. It does this by ignoring all frames whose MAC address doesn't match its own MAC.
- A sniffing program turns off this filter, putting the Ethernet hardware into "promiscuous mode

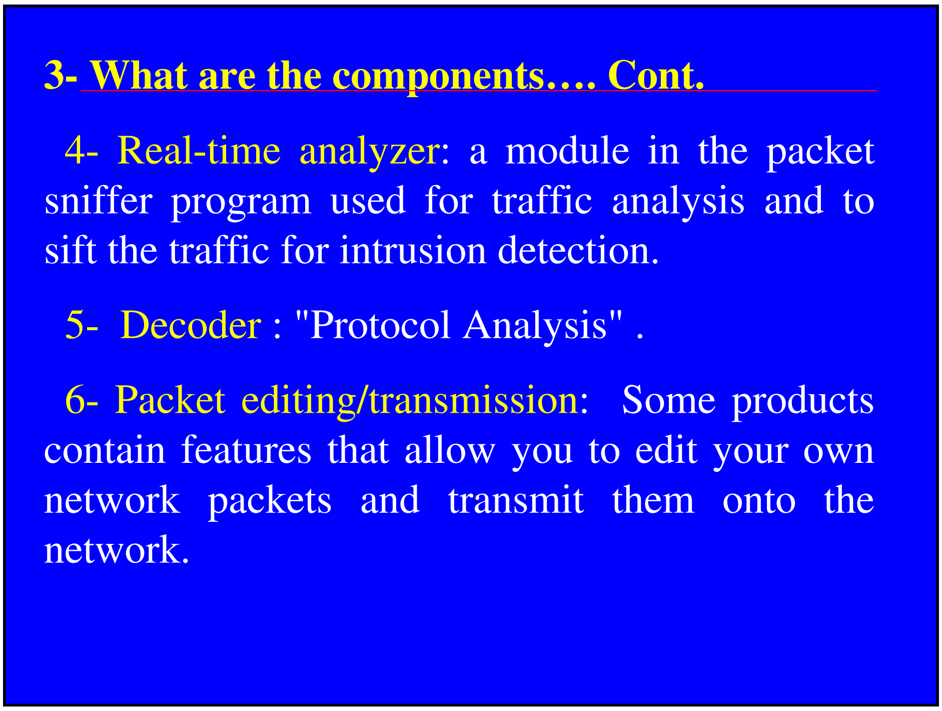


3- What are the components of a packet sniffer?

1- Hardware : standard network adapters .

2- Capture Filter : This is the most important part . It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.

3- Buffers : used to store the frames captured by the Capture Filter .

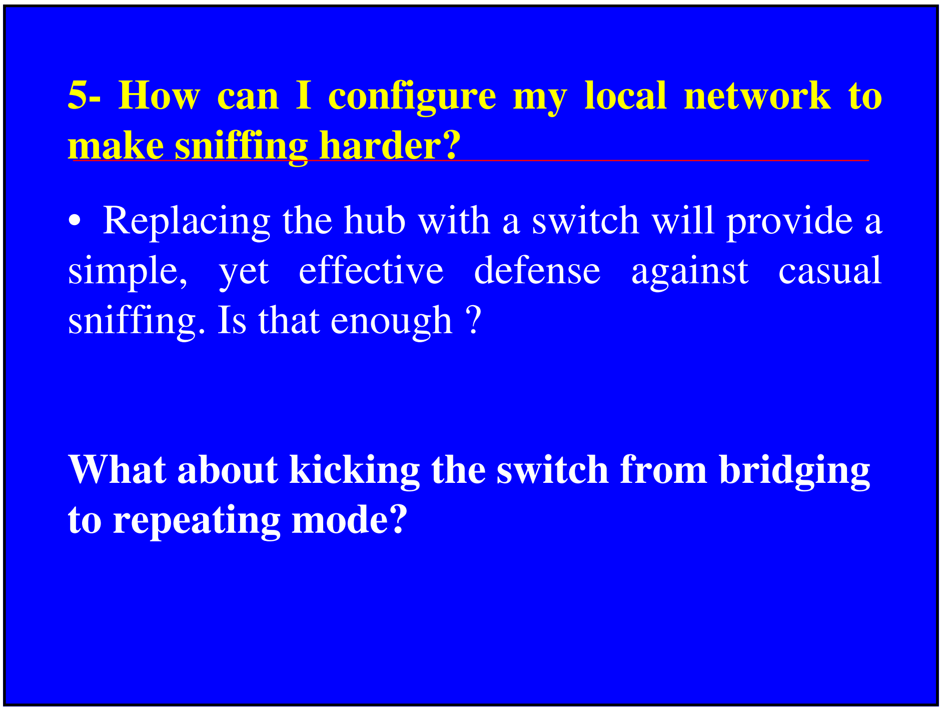


3- What are the components…. Cont.

4- Real-time analyzer: a module in the packet sniffer program used for traffic analysis and to sift the traffic for intrusion detection.

5- Decoder : "Protocol Analysis" .

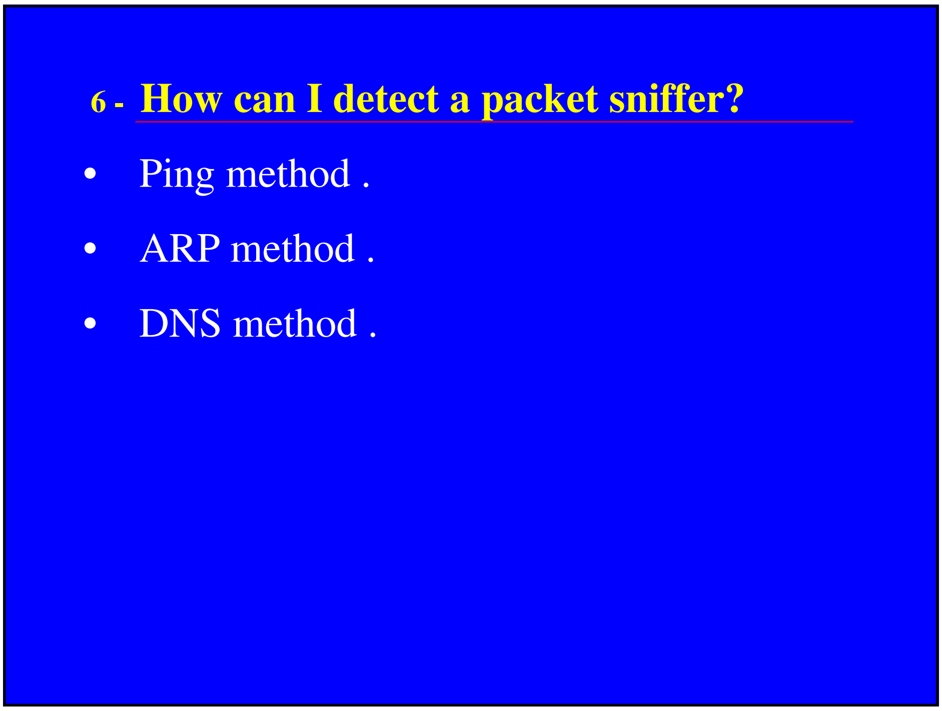
6- Packet editing/transmission: Some products contain features that allow you to edit your own network packets and transmit them onto the network.



5- How can I configure my local network to make sniffing harder?

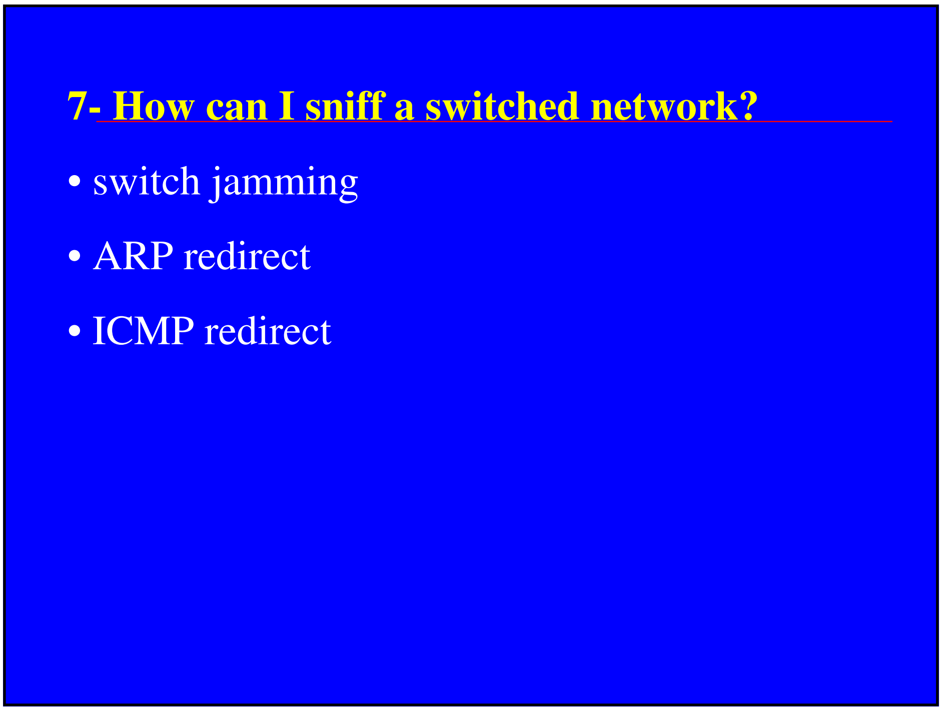
- Replacing the hub with a switch will provide a simple, yet effective defense against casual sniffing. Is that enough ?

What about kicking the switch from bridging to repeating mode?



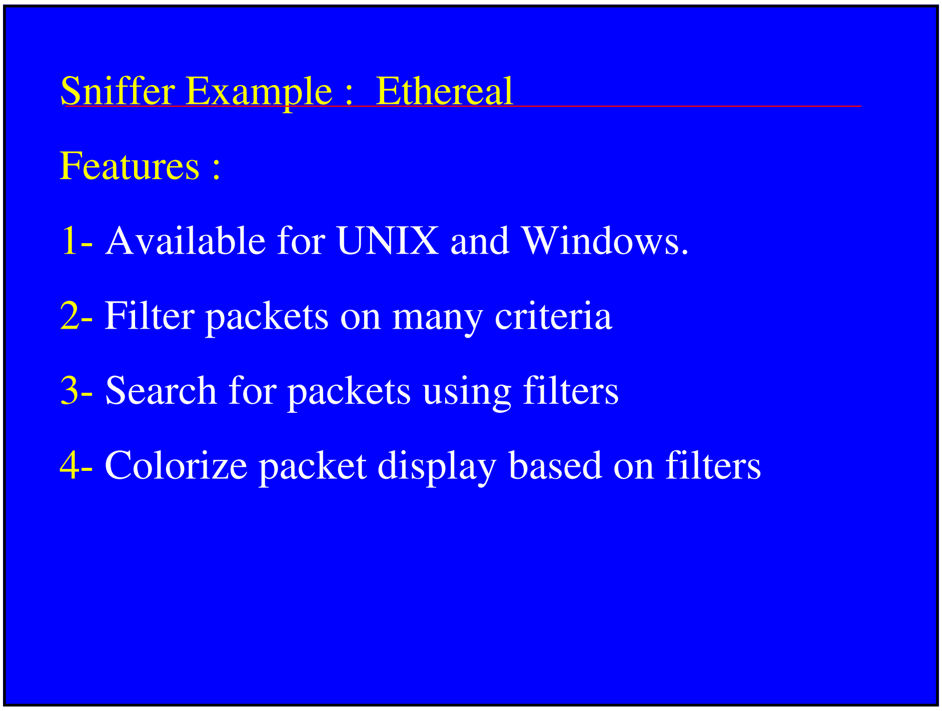
6 - How can I detect a packet sniffer?

- Ping method .
- ARP method .
- DNS method .



7- How can I sniff a switched network?

- switch jamming
- ARP redirect
- ICMP redirect



Sniffer Example : Ethereal

Features :

1- Available for UNIX and Windows.

2- Filter packets on many criteria

3- Search for packets using filters

4- Colorize packet display based on filters