Notes :

Basic Network Sniffer Python

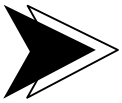
Rana Chouchen

- A sniffer, also known as a packet analyzer or network analyzer, is a tool used to capture and analyze network traffic. It is a software or hardware tool that intercepts and records data packets transmitted between computers or devices on a network.

- Packet sniffers are commonly used for network troubleshooting, security analysis, and network optimization. They can be used to identify network problems such as congestion, packet loss, or improper configurations, and they can also be used to detect security threats such as network intrusions or unauthorized access attempts.

- Packet sniffers work by capturing packets of data as they are transmitted on the network. These packets are then analyzed and displayed to the user in a human-readable format, allowing them to examine the contents of the packets and extract information from them.

- it is important to note that packet sniffers can also be used for **malicious purposes**, such as intercepting sensitive information such as passwords, credit card numbers, or personal information.



A Sniffer is a program or tool that captures information over a network.

2 types

Commercial Sniffers: used to maintain and monitor information over the network

Underground Sniffers : used by hackers to capture information over a network

Components of a Sniffer:

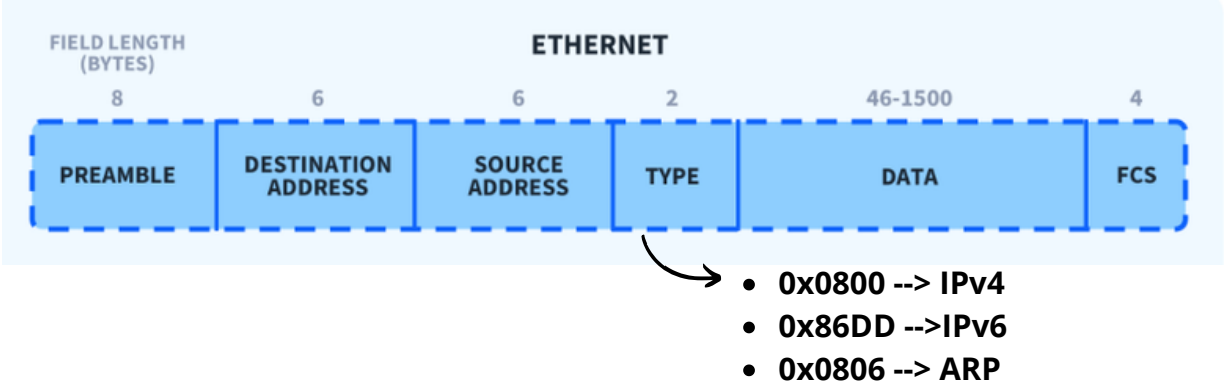
Hardware	Capture Driver	Buffer	Decoder
Sniffers use standard network adapters to capture network traffic.	captures network traffic from Ethernet wire - filters for information - stores the filtered info in a buffer	where data stored : until filled or by replacing	transform the info from binary to readable

Placement of Sniffer:

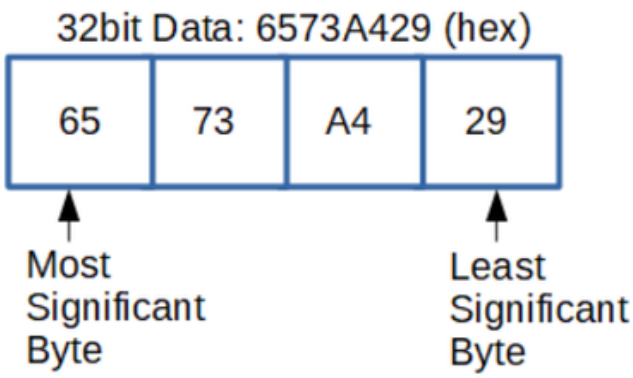
1. Computer
2. Cable wires
3. Routers
4. Network segments connected to the internet

Network sniffers can be operated in two modes.

- **Passive sniffing :**This involves simply listening to and capturing traffic. This type of sniffing is not detectable.
- **Active sniffing :** An Address Resolution Protocol (ARP) spoofing or traffic-flooding attack is launched against a switch in order to capture traffic. This is detectable by network intrusion tools.

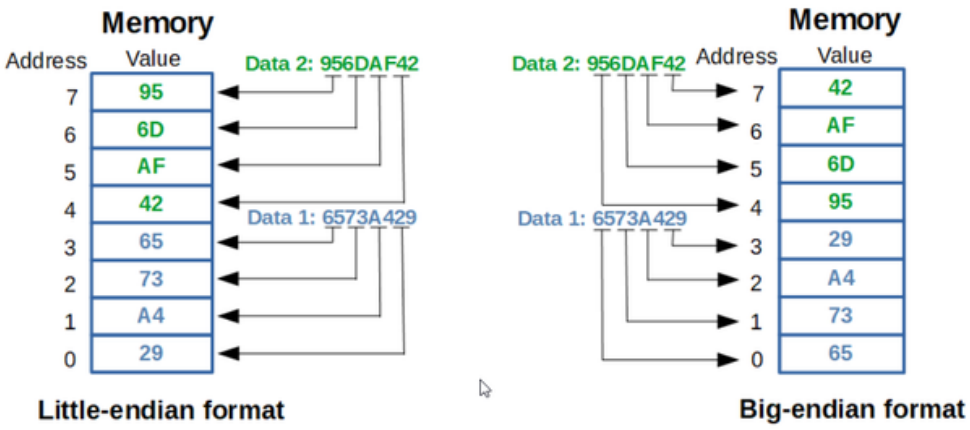


- data transmitted over the network is converted from host byte order to network byte order before transmission and from network byte order to host byte order upon reception.
- Host byte order = little-endian
- network byte order = big-endian
- **Endianness** : refers to the way bytes are ordered when a data item with a size bigger than 1 byte (e.g. 32-bit variable) is placed in memory or transmitted over a communication interface.



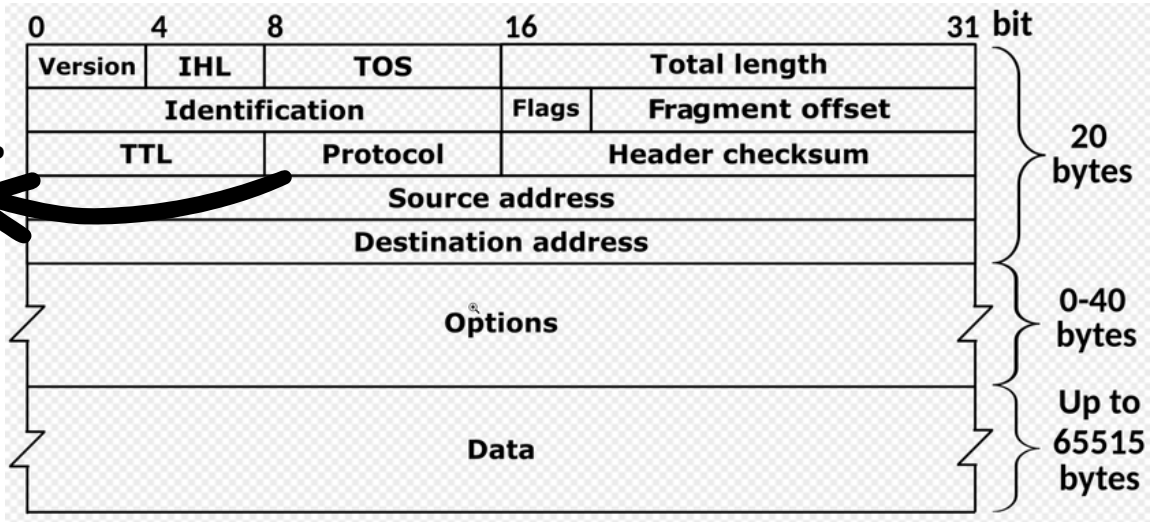
There are two types of endianness:

- **Little-endian** : The bytes are ordered with the least significant byte placed at the lowest address.
- **Big-endian** : The bytes are ordered with the most significant byte placed at the lowest address.

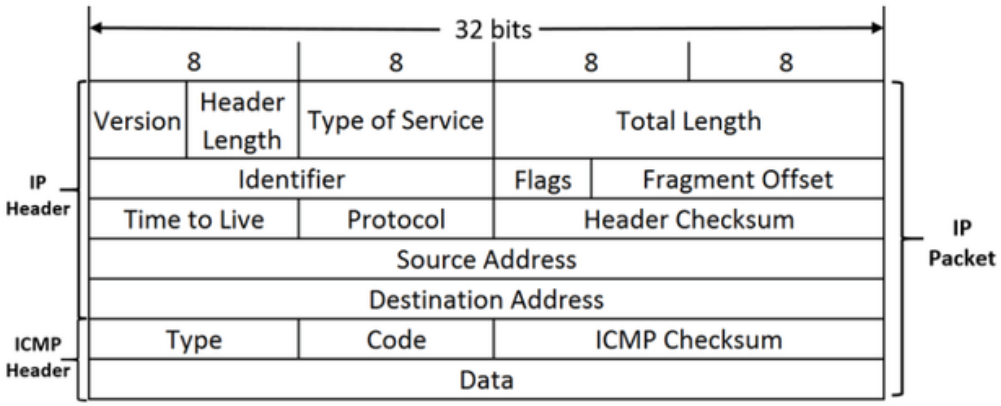


IPv4 Packet :

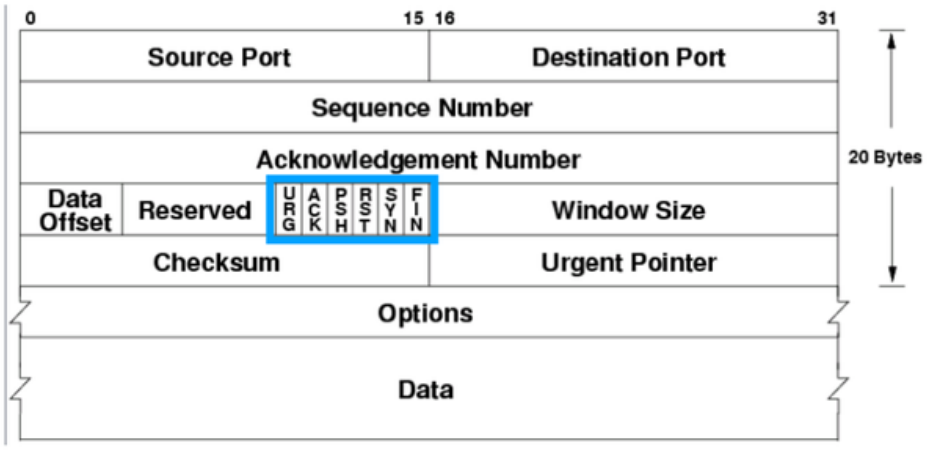
- **1 --> ICMP**
- **6 --> TCP**
- **17 --> UDP**

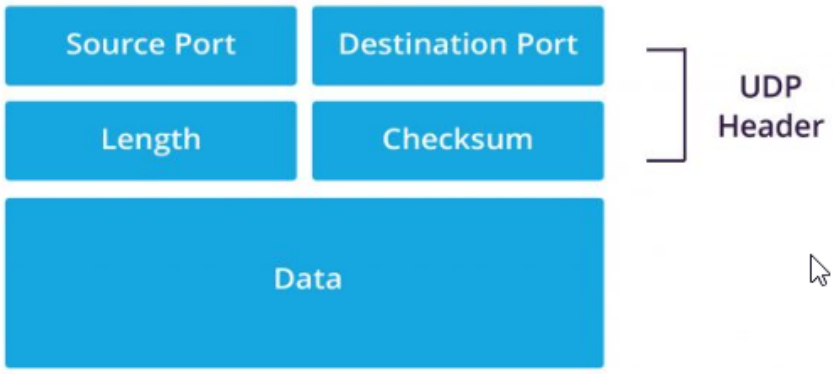


IPv4 Packet (ICMP):



TCP Segment :


0
15 16
31
Source Port
Destination Port
Sequence Number
Acknowledgement Number
20 Bytes
Data Offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window Size
Checksum
Urgent Pointer
Options
Data


Source Port
Destination Port
Length
Checksum
UDP Header
Data