

Practical-4

Aim:

Experiments on packet capture tool: wireshark

Packet sniffer:

- * Sniffs messages being sent/received from/by your computer.
- * Store & display the contents of various protocol fields in the messages
- * Passive program
 - never sends packet itself
 - no packets addressed to it
 - receives a copy of all packets

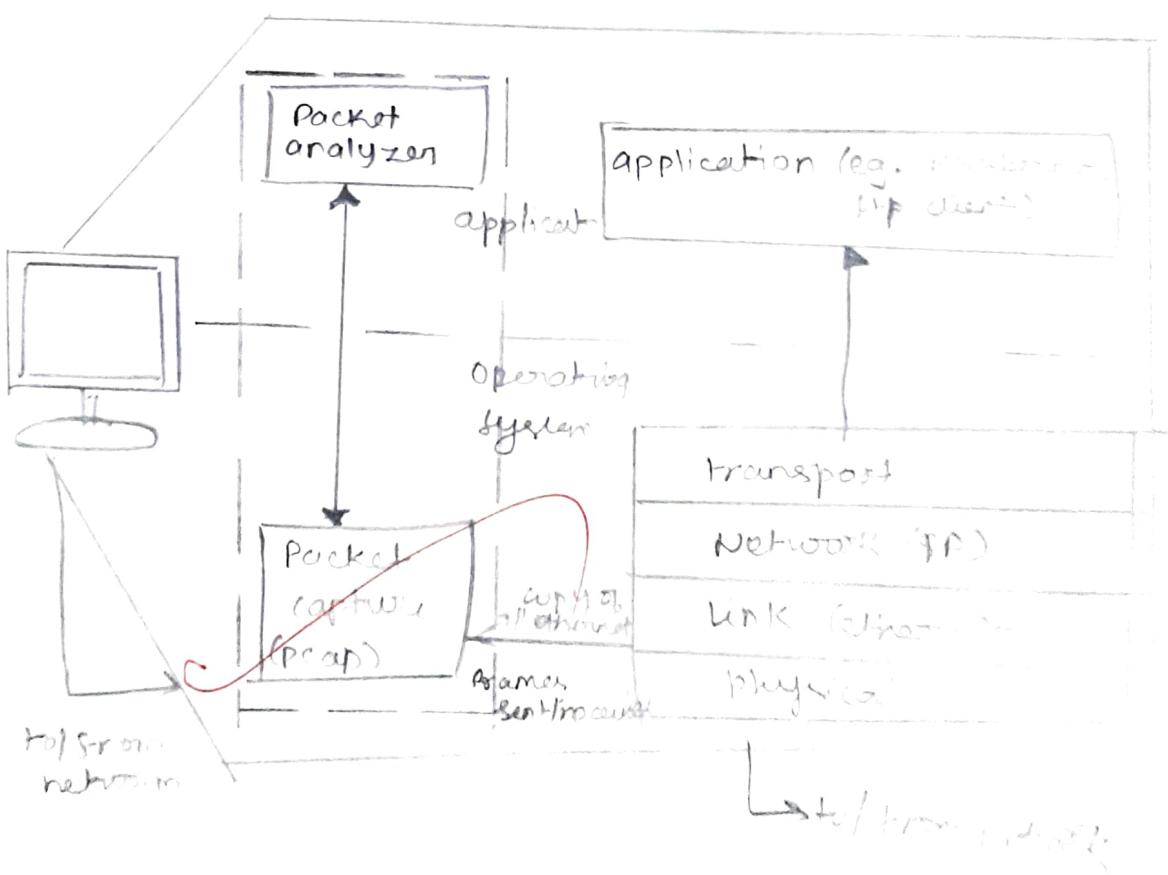
Packet Sniffer structure Diagnostic Tools

* Tcpdump

- E.g. -tcpdump -enx host 10.129.41.2 -W 002302

* wireshark

- wireshark -o file 3.out



Description:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time & display them in human-readable format. Wireshark includes filters, color coding & other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network or troubleshoot network problems.

Q What is promiscuous mode?

Promiscuous mode is a network interface mode that allows a network device - typically a Network Interface Card (NIC) - to pass all traffic it receives to the CPU, not just the traffic addressed to it.

2) Does ARP packets have transport layer header? Explain.

No, ARP packets do not have a transport layer header because ARP operates at the Data Link layer (Layer 2), not the Transport layer (Layer 4). It is used to map IP addresses to MAC addresses & is encapsulated directly in Ethernet frames not in IP, TCP, UDP.

3) Which transport layer protocol is used by DNS?

DNS mainly uses UDP on Port 53. However, DNS also uses TCP for zone transfers or when the response data is too large for UDP.

4) What is the port number used by HTTP protocol?

HTTP uses Port 80 by default

If the site is secured with SSL/TLS then it uses HTTPS on port 443.

5) What is a broadcast IP address?

A broadcast IP address is an address that allows information to be sent to all devices in a network at once.

Eg: In a network 192.168.1.0/24 the broadcast address is 192.168.1.255

All hosts in the sub net receive the packets.

Q1/10/25 %

Result:

Wireshark was used to capture & study network traffic. It showed how data moves between devices. The tool helped understand how the Internet & networks protocols work.