**Performing an initial capture**

When you click on a packet in packet tracer it shows a lot of information about the packet.

The first six character of a source mac address represents the **vender** who owns that group of mac addresses.

**The OSI Model in Wireshark**

When you examine the data in Wireshark it breaks down the layers of the OSI model that way you can see what exactly is going on during a request.

A screenshot of a computer

Description automatically generated

**Learning from Idle Network Data**

Spanning tree protocol helps find the loops in the network. With this if you have a wire that is looped into the same switch it will catch it so broadcasts don’t get looped and kill the network.

* Layer 2 protocol

Which of the following is an industry standard protocol used to identify devices directly connected in a network environment?

* Link Layer Discovery Protocol (LLDP)
  + Discovery directly connected devices.

Cisco Discovery Protocol (CDP)

**Practical Wireshark: ARP | Address resolution Protocol**

A procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN).

Which type of message is an ARP?

* Broadcast

**Practical Wireshark: Rogue DHCP**

If you want to filter down to just DHCP packets in Wireshark, which filter construct can you use?

* DHCP

**Practical Wireshark: DNS**

To test DNS server functionality, which command-line utility can you use?

* nslookup

**Practical Wireshark: Telnet**

Which port number does telnet use?

* TCP – port 23