# Layer 2 Troubleshooting Tools

## Table of Contents

Layer 2 Troubleshooting Tools.................................................................................................................. 2  
Protocol Analyzer ........................................................................................................................................ 3  
Wireshark (Ethereal) ............................................................................................................................ 4  
Network Sniffing - Passive ...................................................................................................................... 6  
Network Sniffing - Active ....................................................................................................................... 7  
Nmap.................................................................................................................................................. 9  
ARP (Address Resolution Protocol) -1................................................................................................. 10  
ARP (Address Resolution Protocol) -2.................................................................................................. 11  
Notices .......................................................................................................................................... 12
Layer 2 Troubleshooting Tools

**019 Layer 2 troubleshooting tools.**
Protocol Analyzer

A hardware or software tool used to capture and analyze signals and data traffic over a communications channel.

The primary benefits over software-based protocol analyzer

- **Mobility** – easily plugged/unplugged and moved
- **Increased capturing throughput** – able to capture information faster and without dropping packets due to data overload, many gigabit networks require a hardware-based analyzer to keep up with line speeds
- **Media flexibility** – provide more network connection options than software-based protocol analyzers, connection possibilities include LAN, WAN, wireless, and circuit-based Telco lines

**020** You can use a hardware or a software tool to help troubleshoot protocols at layer 2. Both a hardware or software tool can be used to capture and analyze signals and analyze data traffic over a communications channel. There's hardware and software for phones—or, excuse me-- there's software for phones and there's individual hardware that exists on its own to analyze protocols at layer 2.

And there's different reasons why we would use one or the other. In my day today I use a piece of hardware to do layer 2 troubleshooting and Wi-Fi analyzing. It's basically-- it's called
a fluke, and it’s a piece of hardware about the size of a brick that I carry around when I go around to new locations and it lets me figure out what the wireless topology is around me. Because I use a piece of hardware just for this purpose, it’s very mobile, right? I don’t have to have it plugged in anywhere, I can take it with me, and it’s very flexible. It’s very nice to use.

**Wireshark (Ethereal)**

Originally called Ethereal – a network protocol analyzer with a graphical user interface (GUI) for both Windows and UNIX/Linux
Captures network traffic off an interface (network card)
Allows for promiscuous mode and passive sniffing
Captures packets without ever sending a packet to elicit a response
Customizable filters
Can reassemble connections/streams

**021** We can use some software-based tools as well. Some of the hardware that we use can implement some software. I know nowadays a lot of phones, you can get apps that
will analyze wireless signals, whether they're cell signals or actual Wi-Fi signals. In this case, the example we're going to talk about is called Wireshark, formerly known as Ethereal. I don't think it's been called Ethereal for-- it's got to be seven or eight or nine years now. So it's been a while.

But Wireshark is a free and open source tool. You can go download it from the internet. It doesn't cost any money, and is a software-based network protocol analyzer that has a user interface that's really easy to work with. If you find yourself at a point in the network where you can capture traffic-- and we'll talk about how that may happen in a couple minutes-- you can use a tool like Wireshark to help analyze that traffic that you captured, figure out who's sending to who, and in some cases decrypt or decode some of the traffic that you receive. It's very, very customizable and definitely one of the better tools out there for doing this type of thing.
Network Sniffing - Passive

Capturing traffic in a hub environment

- Usually sniffer is placed in “promiscuous mode” and listens only.

**022 We would use a tool like Wireshark in an environment where we can capture traffic. If we were doing this on a network in which there was a hub implemented, we can place our sniffer or our network card in what’s called promiscuous mode, also known as monitor mode, and that will allow us to basically receive traffic and analyze it, and not interfere with it, I should say, by sending information. It’s listen-only.
Network Sniffing - Active

Packets captured in a switch infrastructure or where the attacker is actively sending network traffic

- Requires the sniffer to send packets in order to solicit a response, capture response, and potentially poison receiving hosts and/or infrastructure devices with the intent of receiving packets addressed to other hosts

Examples

- ARP Poisoning
- MAC Flooding

**023 That’s passive network sniffing. In active network sniffing, we can actually send information as well. This is injecting packets or frames onto a network to help sniff that network to figure out who else is out there, what are the devices out there, and can I interact or can I interfere, in some cases, with them? If I were a bad person, I’d want to interfere with them.

Some examples of when you may do this. The only two examples we have listed are nefarious examples. I don’t think a network administrator would ever purposefully do something like this. Our ARP poisoning, or Address
Resolution Protocol poisoning, and MAC flooding, or MAC address flooding. Basically these two scenarios are— for the first one, we’ll talk about Address Resolution Protocol flooding, or poisoning, first, which is where you can basically tell a switch that instead of a MAC address—a switch port going to the right MAC address on the correct switch port, you can basically impersonate and tell the switch to send that traffic to your MAC address instead. The way it’s done in practice is a little bit more technical than that, but generally speaking that’s how it goes.

MAC address flooding. With software, you can tell your network interface card to basically identify itself as many different MAC addresses, and when you send that type of traffic to a switch, it doesn’t know what to do and can sometimes be overwhelmed, overloaded, and fill up your CAM table on your switch and then you get problems, especially if that happens for an extended period of time. It causes the memory of the switch to become overloaded and in some cases can cause significant slowdown in a network segment, and that’s MAC flooding.
Nmap

A very powerful, free, open source tool for network scanning

- Port scanning, OS detection, version detection, ping sweep, and more
- Ability to scan a large number of machines at once
- Supported by numerous operating systems

**024 Another great tool we can use for analyzing networks at layer 2 is Nmap. Nmap is a free and open source tool. I use this all the time in my day-to-day work. It's mainly used for layer 3 and above. You can scan networks, you can discover protocols, you can discover what services are listening on different ports and things like this, but it does have some use at layer 2 as well. You can ARP scan a network. Basically you can figure out what other addresses, what other layer 2 addresses exist on your network with a tool like Nmap.**
ARP (Address Resolution Protocol) -1

Allows the network to translate IP addresses to MAC addresses
Requests MAC addresses for a given IP address
Maintains a local cache for faster responses
Broadcast messages: “Who has 192.168.1.5, tell 192.168.1.1”
  • Response to the broadcast is a MAC address.
No authentication – very easy to spoof MAC addresses in cache
  • First response to an ARP request gets in the cache
  • Setup for Man-in-the-middle attacks, ARP poisoning

**025 And Address Resolution Protocol.
ARP (Address Resolution Protocol) -2

Each device creates a local ARP table matching IP to MAC addresses as they are identified to the host.

Switches create CAM tables linking MAC addresses to its physical ports.

“arp –a” shows local arp cache.

```
C:\Windows\system32>arp -a

Interface: 10.192.168.50 -- 0x8b
Internet Address  Physical Address  Type
10.192.168.12   74-64-01-39-94-96  dynamic
10.192.168.52   00-12-3f-7a-63-f0  dynamic
10.192.168.53   00-8d-6b-bb-12-9b  dynamic
10.192.168.54   00-13-68-79-77-8d  dynamic
10.192.168.55   00-19-bb-f0-04-f6  dynamic
10.192.168.56   60-6b-bd-40-32-66  dynamic
10.192.168.57   00-8d-6b-bb-12-9b  dynamic
10.192.168.58   00-1a-29-3a-38-0d  dynamic
10.192.168.59   00-10-7f-2a-2f-fc  dynamic
10.192.168.60   00-1a-29-3a-38-0d  dynamic
10.192.168.61   ff-ff-ff-ff-ff-ff  static
```

**026 And a Windows demonstration of showing your ARP table.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.