Monitoring network traffic in a small network

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

Contents

- Tapping into the wire
- Introduction to Wireshark
- Working with captured packets

Tapping into the wire

- Living promiscuously
- Hubs and switches
- Sniffing a routed environment

Living promiscuously

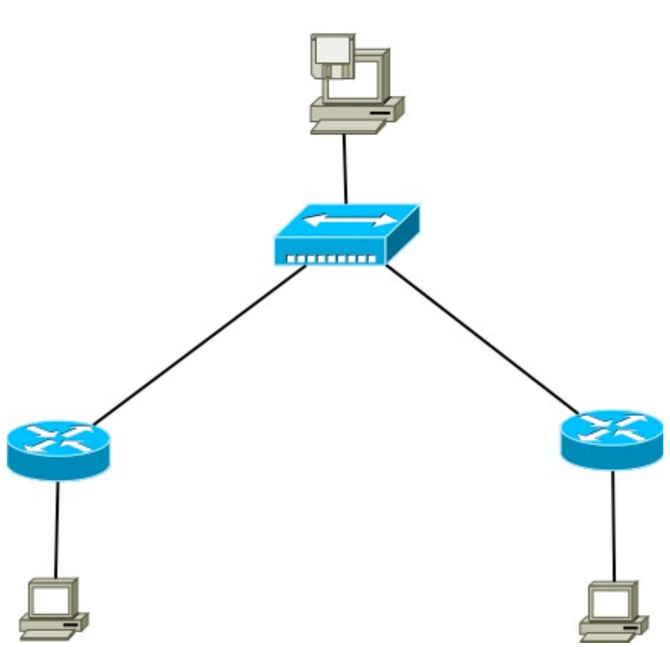
- View all packets coming into the NIC
- Passes all captured traffic to the CPU
- Basically all sniffing requires promiscuous mode

Hubs and switches

- On a hub you receive all traffic, even traffic not addressed to your computer
- On a switch you only receive traffic destined to your NIC
- Sniffing a switch usually requires *port mirroring*

Sniffing a routed environment

- The importance of where to sniff



Introduction to Wireshark

- History
- Benefits
- A quick demo

Working with captured packets

- Finding and marking packets
- Saving and exporting capture files
- Time display formats and references
- Capture and display filters
  - http://wiki.wireshark.org/CaptureFilters