A Short Intro to Wireshark

About

- WireShark is a packet analyzer
  - also packer sniffer
- What does Wireshark do?
  - it captures packets on the NIC (Network Interface Card)
  - analyzes the protocol headers
  - filters packets according to your preferences
  - displays packets with time stamps, headers, content and helpful information
    - protocol, flows, timing, etc.
  - provides tool to analyzes your traffic

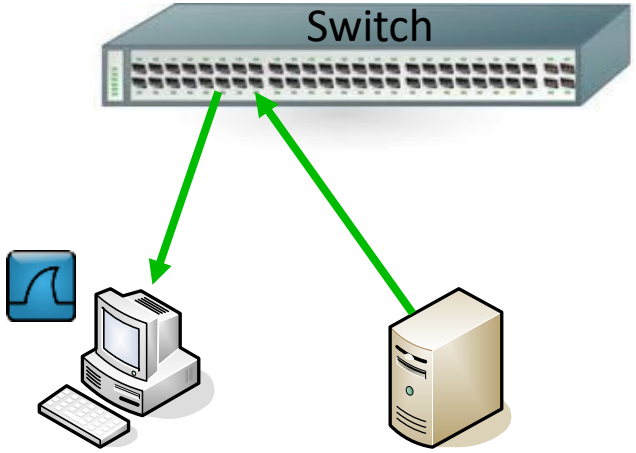
What is Wireshark good for?

- Every Internet user
  - investigate with whom your computer/your programs/your browser is communicating
  - understand your network performance and investigate potential performance problems
    - Why is the connection to a server so slow?
- Developer of networking applications
  - debug your code by analyzing the exchanged packets
  - check for network-originated performance problems
- Network administrator / network operator
  - check for network problems
  - identify misbehaving computers and attacks from within or outside the network

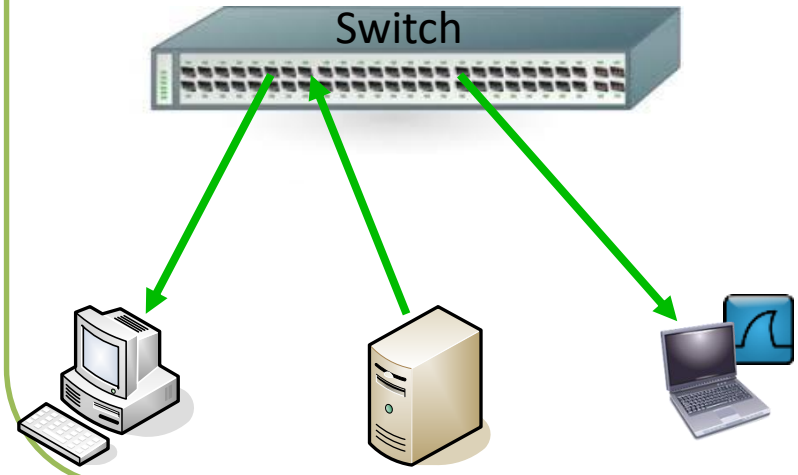
Collecting Packets

On the client:

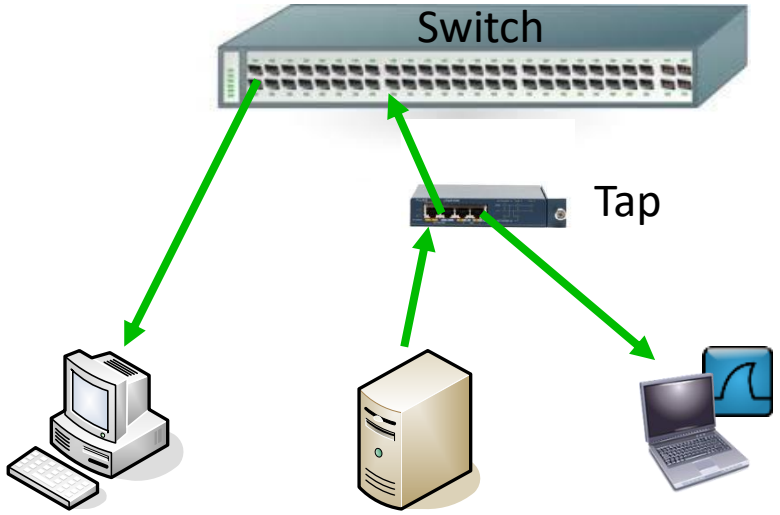
- only sees packets to/from the client's address and broadcast traffic
- cannot sniff other traffic in the network



Span/Mirror: Switch copies selected ports, hosts, vlans, or traffic patterns to a monitor port



Tap: Device that forwards traffic and puts a copy on another port



What can you analyze with Wireshark

- Standard usage:
  - live traffic on Ethernet or WiFi NIC
  - you may deploy capture filter to reduce the number of packets stored by WireShark
- Analyze traffic dumped in a file:
  - you can dump traffic into a file using command line applications like tcpdump or rawcap that run in the background and analyze the file later
  - you can use rawcap to dump computer internal (localhost) traffic to a file and, rawcap needs admin rights
- Other types of traffic
  - Wireshark also supports PPP (DSL), DOCSIS (cable modem), USB, or Bluetooth traffci

And now try it …