Lab 8: SNMP

15 points

**Due: Before class on 4/20/2022**

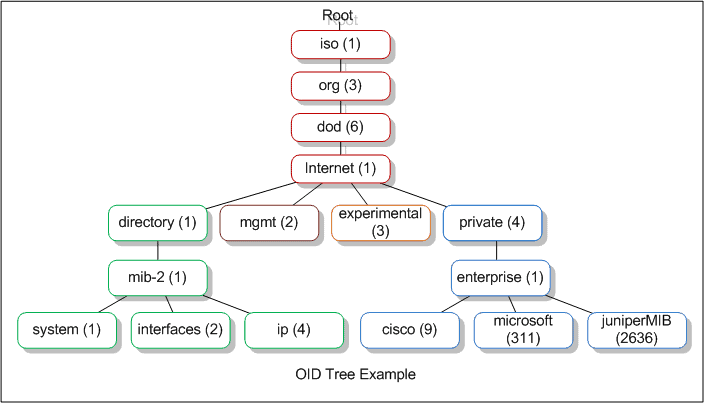
**Objectives of this lab:**

1. Learn about aspects of SNMP by analyzing pcap files with Wireshark
2. Research aspects of SNMP

# PCAP file 1

For the following questions open the file **snmp.pcap** from the D2L lab.

As discussed in class, when querying SNMP you can request or get information by the corresponding MIB. MIBs are formatted like trees:



Source: <https://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics/>

Most MIBs will start out with either: 1.3.6.1.2 (for network management interfaces) or 1.3.6.1.4.1 (for private company created interfaces), the numbers after that are defined by the vendor.

1. SNMP has multiple versions, look under the “Simple Network Management Protocol” dropdown in the Details pane. What version of SNMP is being used in this file? [1 point]
2. In the same section of the PCAP file there is a key labelled “community”. What is the value of this key? [1 point]
3. What is the community string used for in SNMP? [1 point]
4. What protocol (TCP/UDP) and ports does SNMP use? (There are 2 ports used by SNMP but you will only find 1 of them in this capture.) [3 points]
5. We discussed in class (and you can see in the pcap) that SNMP uses sets of request/replies to get data from a network host. If you fetch a lot of data with SNMP, is it guaranteed that the data will all be collected at the same time and be consistent (i.e., values will “add up” if they’re related)? Why or why not? [2 points]

# PCAP file 2

For the following questions open the file **snmp2.pcap** from the D2L lab.

1. What is the value of the community string in this capture? [1 point]
2. What version of SNMP is used in this capture? [1 point]
3. What are the differences between the SNMP version used in the first capture and this capture? [2 points]
4. The most current version of SNMP is SNMPv3, what are the benefits and drawbacks to using the most current version? [3 points]