# Introduction to SNMP

AfNOG 11, Kigali/Rwanda




Google™

# What is SNMP?

- SNMP - **S**imple **N**etwork **M**anagement **P**rotocol
- Industry standard protocol to manage network equipment
  - Mostly routers/switches support it, but also PCs, Firewalls and some other equipment
- Manager (monitoring/management station) communicates with agents (monitored/managed devices)
  - Either manager requests information or changes (GET/SET) --- we focus on GET
  - Or Agent tells manager something happened (TRAP)
  - Management Information Base (MIB) defines variables maintained by the agent

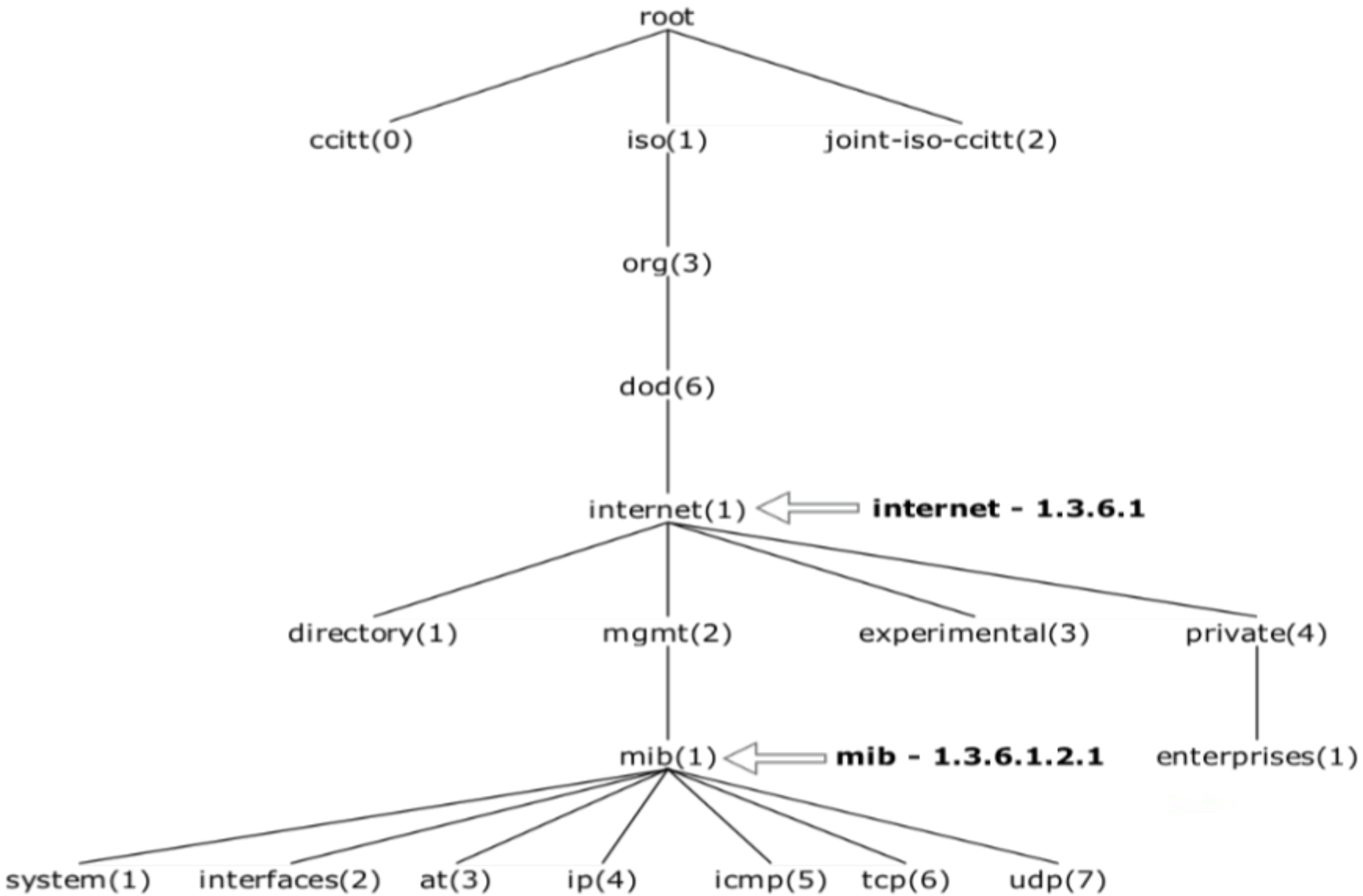
# How does SNMP work?

- Communication on UDP Port 161 (unreliable!)
- Used mostly for monitoring
  - Interface usage bytes / packets / errors
  - Environmental: Temperature,CPU,Disk
  - Protocols: e.g. OSPF neighbour status
  - Caveat: not everything you can get via other methods, you can also get via SNMP!
  - Tools in this class: Nagios/Cacti use SNMP extensively
- Variables in MIB are identified by object identifiers (OIDs)
  - Hierarchical naming
  - Standard variables (system/interfaces/etc) and vendor specifics (e.g. Cisco)

# Types of packets

- *GetRequest* - request information about a certain variable
- *GetNextRequest* - get next variable after a certain OID
- *SetRequest* - set information of certain variable
- *GetResponse* - response to previous three packets
- *Trap* - something happened, this is what (UDP port 162)
  - take care, this is also unreliable
- authentication via "community" (cleartext password)

# MIB tree


root
ccitt(0)
iso(1)
joint-iso-ccitt(2)
org(3)
dod(6)
internet(1)
internet - 1.3.6.1
directory(1)
mgmt(2)
experimental(3)
private(4)
mib(1)
mib - 1.3.6.1.2.1
enterprises(1)
system(1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
udp(7)

# OID and MIBs

- Navigate MIB tree, separated by MIB, each OID has label
- e.g. .1.3.6.1.2.1.1.3 is .iso.org.dod.internet.mgmt.mib.system.sysUpTime
- translation/more information for tools via MIB files, some come with distribution, vendor extensible -- structure in ASN.1 language
- When querying there are simple objects (add .0) or tables (e.g. interfaces - Name/IP/byte counter) with indices

# Different SNMP versions

- SNMPv1 - simple authentication (cleartext password), basic commands
- SNMPv2 - new requests (GETBULK for faster requests, and INFORM for reliable information), new data types (64 bit counters!) and new, complicated security
  - more common v2c, with the old security model
- SNMPv3
  - Current IETF standard: adds authentication, privacy, access control
- You probably want to firewall SNMP at network edges and on the boxes (esp. if you use v1 or v2c)

# Let's try this out

- Unix tools to query SNMP:
  - snmpget
  - snmpstatus
  - snmpwalk
  - snmpset

- Syntax:
  snmpxxx -c community -v1 (-v2c) host [oid]
  (or man snmpget)

- Example:
  snmpget -c afnog -v2c 196.200.218.254 interfaces.ifDescr.0
  snmpget -c afnog -v2c 196.200.218.254 .1.3.6.1.2.1.2.1.2.2
  snmpwalk -c afnog -v2c 196.200.218.248 system

# Exercises

Exercises