Simple Network Management Protocol (SNMP)

November 2016

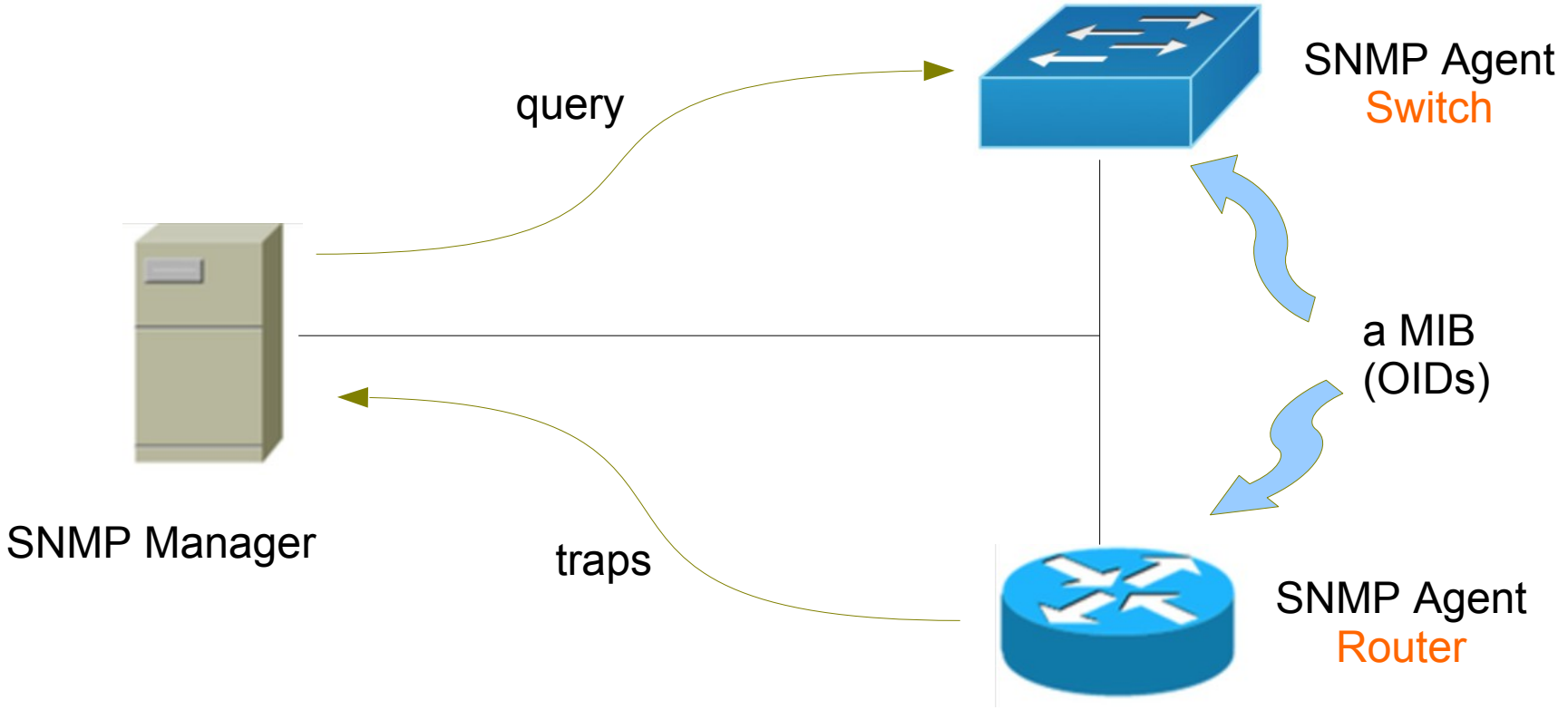
Kandy, Sri Lanka

Senevi Herath
(LEARN)

Overview

- What is SNMP?
- Polling, querying and traps
- SNMP versions
- SNMP roles
- How does SNMP work?

What is SNMP


query
SNMP Agent
Switch
a MIB
(OIDs)
SNMP Manager
traps
SNMP Agent
Router

Simple Network Management Protocol

- What is SNMP?
  - structured protocol, structured information
  - Used to queering network device state and receiving notifications (traps)
  - Can be used to change state
  - Industry standard, hundreds of tools exist that
  - Supported on any decent network equipment
  - Transport: UDP port 161 and 162 (traps)

- Uses for SNMP?
  - Typical queries
    - Bytes In/Out on an interface, errors
    - CPU load, uptime
    - Temperature, disk space
    - Installed firmware/software
    - …..

SNMP Versions

- v1 (1988) original specification
  - Historic, no security, community string (had same default community string)
- v2 (1996) failed standard
  - Security got lot tighter, difficulty to setup
  - Security, new data types, new operators
  - 64-bit counters, get-bulk, v2 notifications
  - View-based access control model (VACM) introduced
  - Historic, no current implementation left
- v2c (1996) de facto standard
  - v2 data types and operators
  - v1 security (community string) – simple security model
- V3c (1998) robust security
  - User/view based security (USM/VACM), Encryption, authentication and authorization
  - Full Internet standard

SNMP roles

- SNMP Manager
  - Sometimes know as the SNMP client
  - SNMPv3 calls it the Command Generator and Notification (trap) Receivers
- SNMP Agent
  - Sometimes know as the SNMP server
  - SNMPv3 calls it Command Responder and Notification Originator

How does SNMP work?

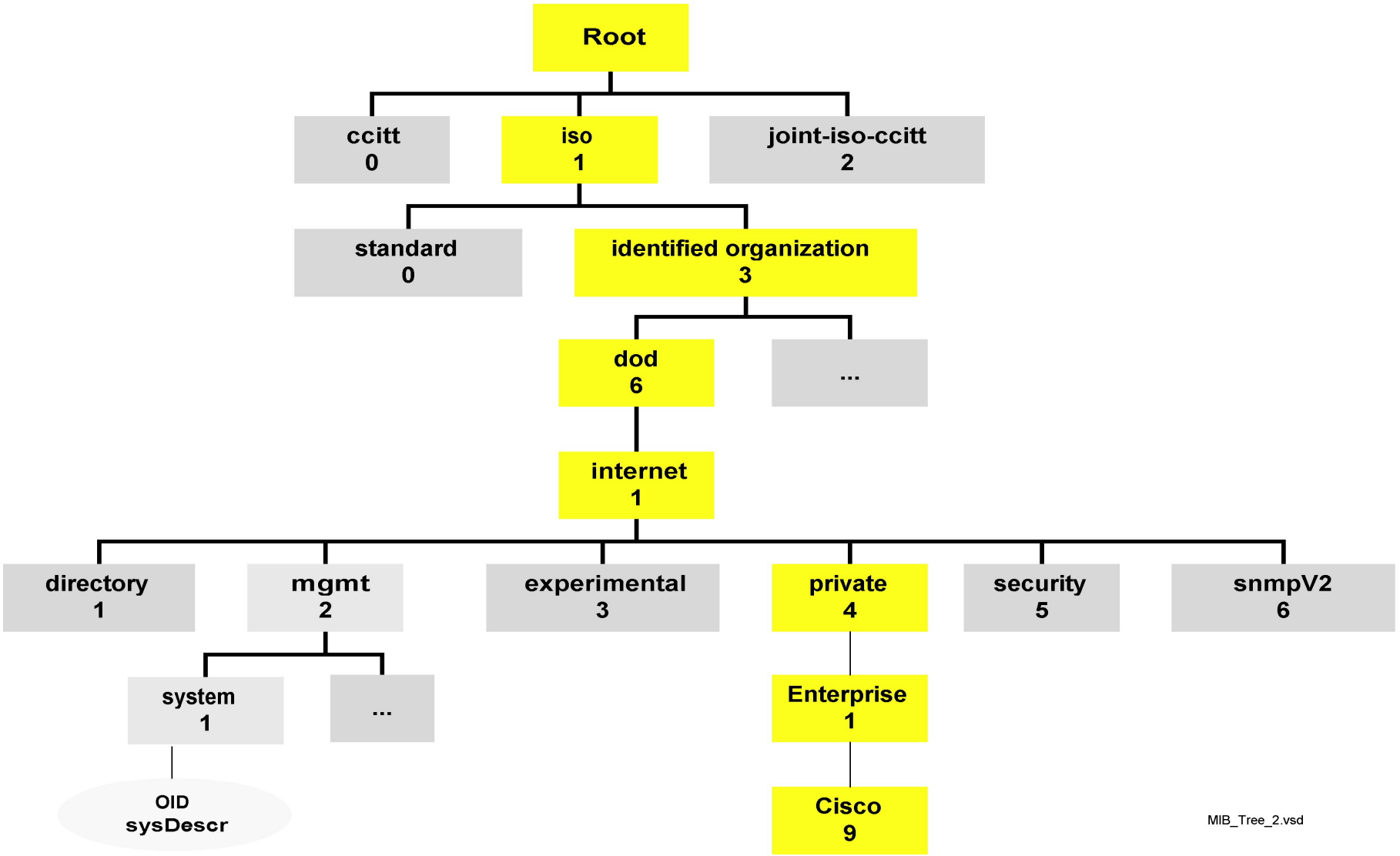
- Basic operators
  - **get** (manager → agent)
    - Query for a value
  - **getnext** (manager → agent)
    - Get next value (e.g. list of values of table)
  - **getresponse** (agent → maneger)
    - Response to get, getnext, or set, includes error returns
  - **set** (manager → agent)
    - Set a value, or perform an action
  - **trap** (agent → manager)
    - Spontaneous notification from equipment (line down, temperature above threshold,..)

The SNMP database

- The information offered by a device is available in its Management Information Base (MIB)
  - SNMP uses Object Identifiers (OIDs) to organize this information
  - OIDs are keys to identifying each piece of data
  - OIDs are organized into a tree structure that is the MIB
  - MIB files document parts of the MIB on a device

- Object Identifier (OID)
  - A unique key to select a particular item of data in the device
  - The same piece of information is always found at the same OID
  - An OID is a variable-length string of numbers, e.g.
    - .1.3.6.1.2.1.1.3
  - Allocated hierarchically in a tree to ensure uniqueness (similar to DNS)

The MIB Tree


Root
ccitt
0
iso
1
joint-iso-ccitt
2
standard
0
identified organization
3
dod
6
...
internet
1
directory
1
mgmt
2
experimental
3
private
4
security
5
snmpV2
6
system
1
...
Enterprise
1
OID
sysDescr
Cisco
9
MIB_Tree_2.vsd

MIB

- Interesting part of the MIB tree
  - The Internet MIB .1.3.6.1, really only two branches interest
    - Standard MIBs
      - .1.3.6.1.2.1 = .iso.org.dod.internet.mgmt.mib-2
    - Vendor-specific (proprietary) MIBs
      - .1.3.6.1.4.1 = .iso.org.dod.internet.private.exterprises
- OIDs and MIB files
  - OID components separated by '.'
    - .1.3.6.1.4.1.9. ….
  - Each OID corresponds to a label
    - 1.3.6.1.2.1.1.5 => sysName
    - .iso.org.dod.internet.mgmt.mib-2.system.sysName
- How do we convert from OIDs to Labels (and vice versa)?
  - Use the **MIBs files** !

Querying an SNMP agent

- Examples
  - snmpstatus -v2c -c LEARN 192.248.1.1
  - snmpget -v2c -c LEARN 192.248.1.1 ifIndex.1
  - snmpwalk -v2c -c LEARN 192.248.1.1 ifDescr