OpenNMS 101

Tarus Balog
tarus@opennms.org
http://www.opennms.org/Training

Module 6: Simple Network Management Protocol (SNMP)

Simple Network Management Protocol

- In OpenNMS, SNMP is a service and more
- The Simple Network Management Protocol (SNMP) is used to gather performance data
- It can also me used to monitor the status of a service.
- The Net-SNMP Agent can be extended to add a lot of useful features

Management Information Base (MIB)

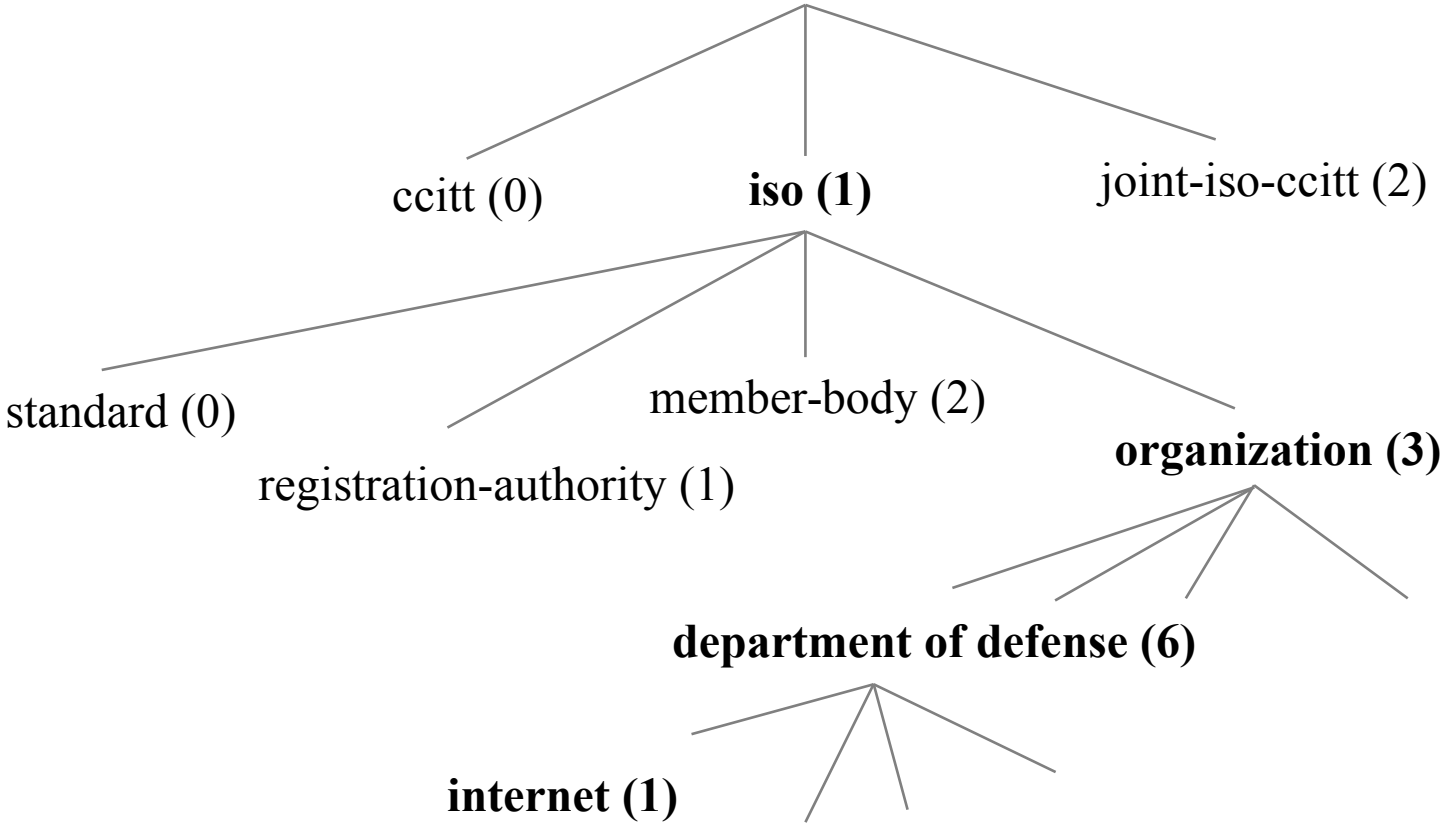
- Data Structure Written in Abstract Syntax Notation (ASN.1)
- Internet Network Management Framework, RFC 1052 (April 1989)
  - Structure of Management Information (SMI), RFC 1065
  - Management Information Bases, RFC 1066
  - Simple Network Management Protocol, RFC 1067

(All August 1988)

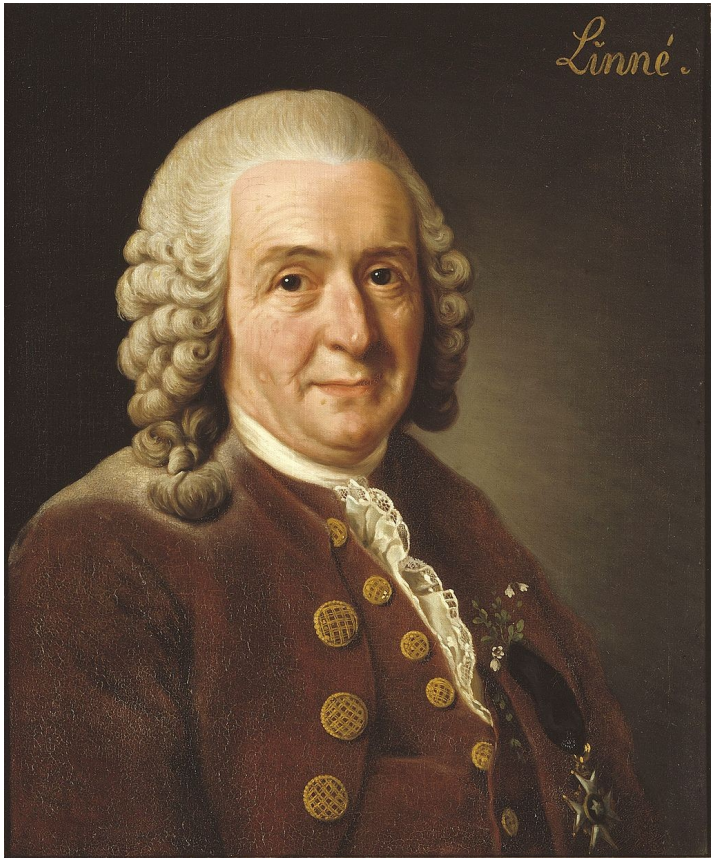
Types of Data Objects

- Integer
- String
- Counter
- Gauge
- TimeTicks (hundredths of a second)

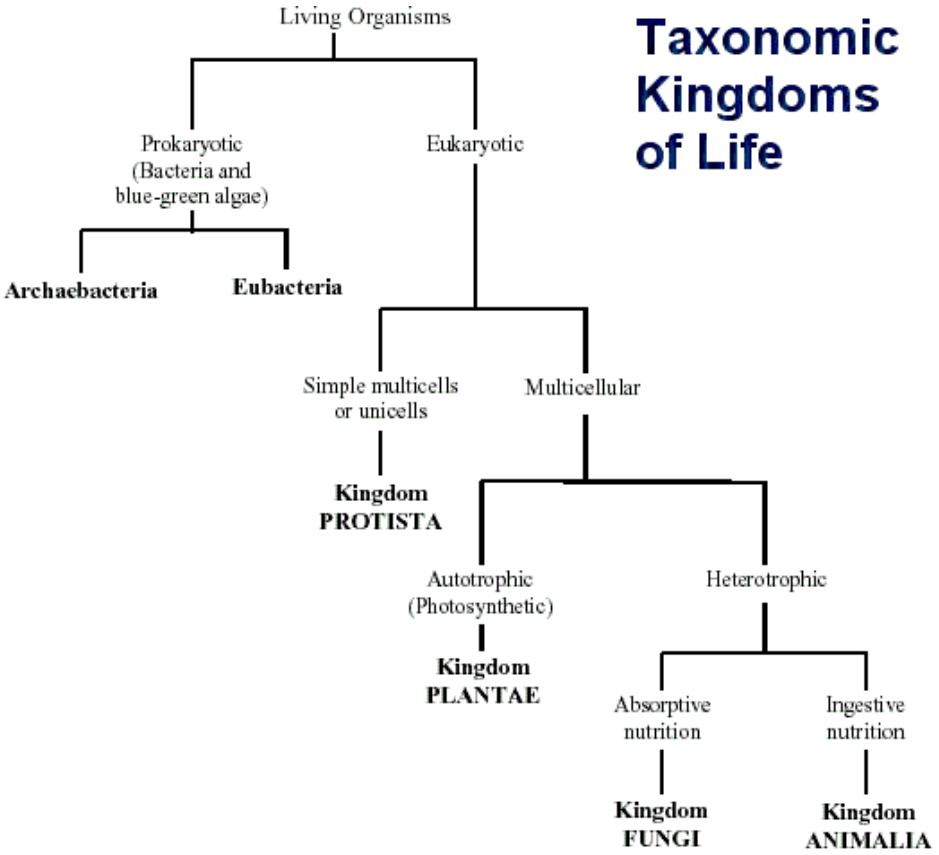
OID Tree Structure



Carl Linnaeus

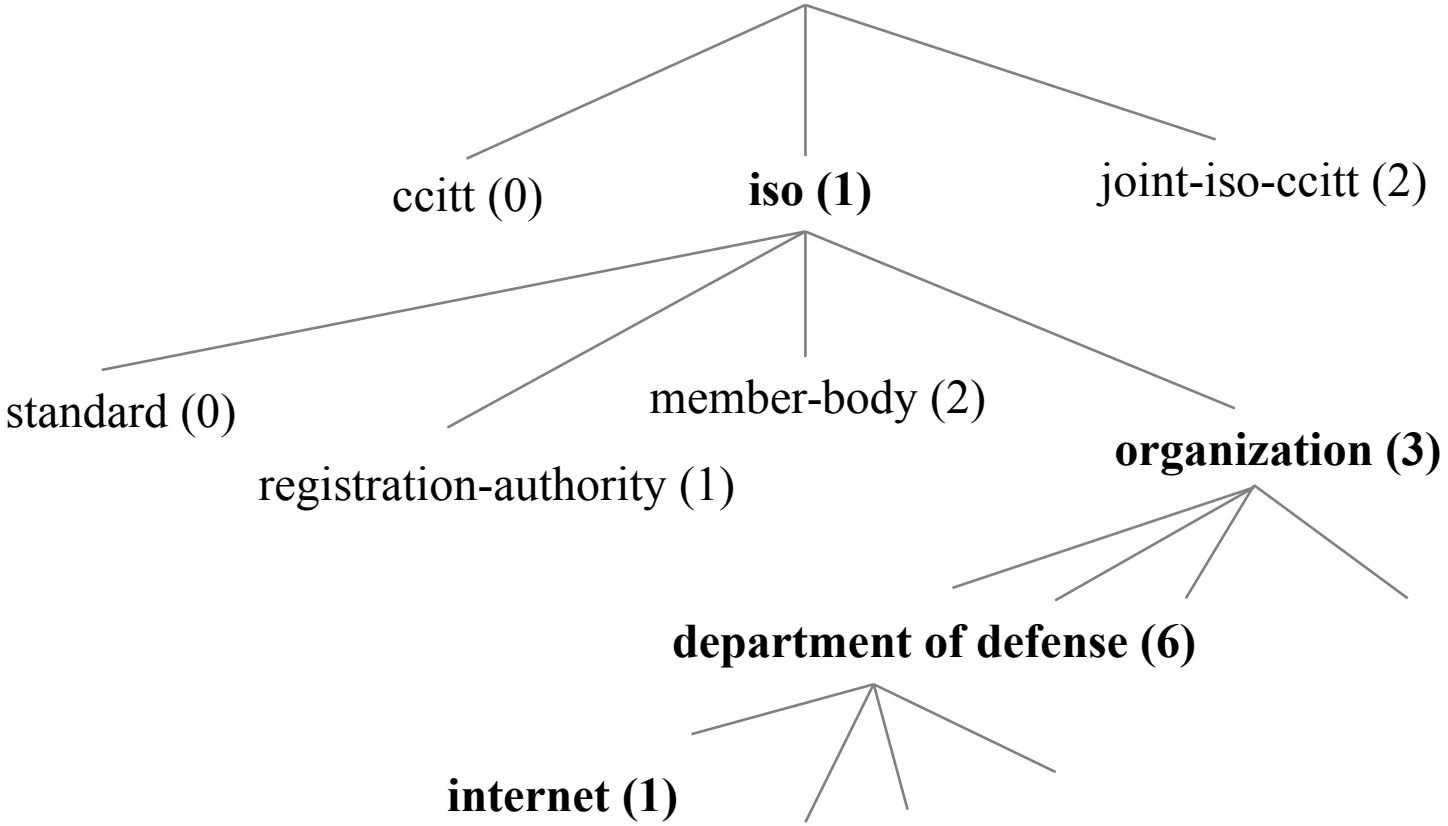


Tree of Life

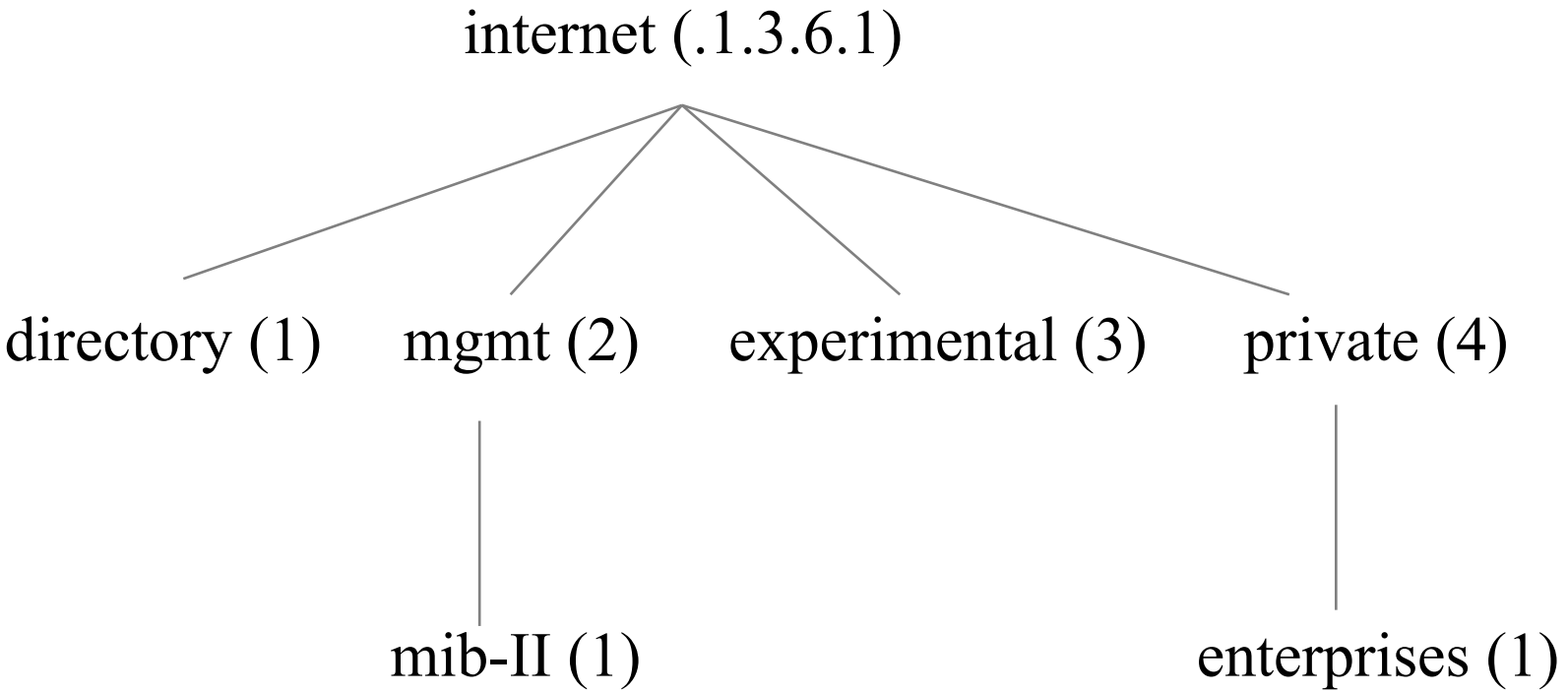


Taxonomic Kingdoms of Life

OID Tree Structure



Internet OID Subtree



MIB-II

- See Handout
- Scaler: ends in “0”

  sysDescr - `.1.3.6.1.2.1.1.1.0`
- Tabular: ends in a non-zero series of numbers

  ifDescr - `.1.3.6.1.2.1.2.2.1.2.3`

  Description of the 3rd interface (index 3 in the ifTable, second object, which is the interface description)

ifTable

ifTable .1.3.6.1.2.1.2.2

ifEntry .1

IfIndex (.1)	IfDescr (.2)	IfType (.3)	MTU (.4)	IfSpeed (.5)
3	fxp2	6	1514	0
4	lsi	150	1496	0
6	lo0	24	2147483647	0
7	tap	1	2147483647	0
8	gre	131	2147483647	0
9	ipip	131	2147483647	0

ASN.1 Example

```
sysDescr OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A textual description of the entity.  This value should
            include the full name and version identification of the
            system's hardware type, software operating-system, and
            networking software."
    ::= { system 1 }
```

Private Enterprise MIBs

- Under the private.enterprises OID subtree .1.3.6.1.4.1
- Numbers assigned by the Internet Assigned Numbers Authority (IANA)
- Common numbers:
  - IBM (2)
  - Cisco (9)
  - HP (11)
  - OpenNMS (5813)
- For more info, see https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

Private Enterprise MIBs

IBM RS/6000:	.1.3.6.1.4.1.2.3.1.2.1.1.2
HP 9000/800	.1.3.6.1.4.1.11.2.3.2.3
HP 9000/700	.1.3.6.1.4.1.11.2.3.2.5
Microsoft Windows	.1.3.6.1.4.1.311.1.1.3.1
Bay Networks 28K Switch	.1.3.6.1.4.1.45.3.15.1
Wellfleet Router	.1.3.6.1.4.1.18.1.1
Net-SNMP on Linux:	.1.3.6.1.4.1.8072.3.2.10

SNMPv1: Five Commands

- GetRequest
- GetResponse
- GetNext Request
- SetRequest
- Trap

SNMPv1: Problems

- Security
  - Community names:
    - Public (read only)
    - Private (write only)
    - Other
  - Device based security
- UDP is connectionless
- Limited to 32-bit Counters

SNMPv2

- 400 pages in RFCs 1441-1452 (April 1993)

  Jeffery Case, Keith McCloghrie, Marshall Rose, Steve Waldbusser
- Results:
  - consensus documents RFCs 1902-1908 (January 1996)
  - SNMPv2C (community based) RFC 1901 (January 1996)
- SNMP version 3 RFC 2570 (April 1999)

SNMPv2: Results

- New data types:
  - BITS
  - Integer32
  - Counter32
  - Gauge32
  - Counter64
- New commands:
  - GetBulkRequest (large amounts of data)
  - InformRequest (manager to manager)

SNMPv3: Results

- SNMP v3 is SNMPv2c with security
- Can encrypt:
  - Authentication
  - Payload
  - Both
  - Neither

net-snmp

- Powerful open-source SNMP agent
- Usually configured in `/etc/snmp/snmpd.conf`
- Must edit for permissions
- OpenNMS requires mapping from `ipAddrTable` to `ifTable`.
- Install with
  `yum install net-snmp net-snmp-utils`

snmpd.conf

```
####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  default       public
com2sec onmsUser       default       YrUsonoZ

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1            notConfigUser
group   notConfigGroup v2c           notConfigUser
group   onmsGroup      v1            onmsUser
group   onmsGroup      v2c           onmsUser
```

snmpd.conf (cont)

```
####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1
view    allview       included   .1

####
# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write  notif
access  notConfigGroup ""      any       noauth    exact  systemview none none
access  onmsGroup      ""      any       noauth    exact  allview    none none
```

snmpd.conf (cont)

```
# It is also possible to set the sysContact and sysLocation  # system variables
through the snmpd.conf file:

syslocation Classroom, Raytheon, 22110 Pacific Blvd., Sterling,
            Virgina, 20166, United States, North America, Earth
syscontact  Tarus Balog <tarus@opennms.com>
```

At the bottom of the file, add:

```
# Destination for traps
trapsink 127.0.0.1

# Disks
disk /
disk /boot
disk /vagrant
```

Then run, as root, `systemctl restart snmpd`

Exercise #6: Configure net-snmp

- Edit the snmpd.conf file to allow for access to anything below .1
- Restart the SNMP daemon.
- Test access via community string
- Update community string in OpenNMS
- Rescan the localhost node

Test Community Strings

Run an snmpwalk with “public”:

```
snmpwalk -v2c -c public localhost .1
```

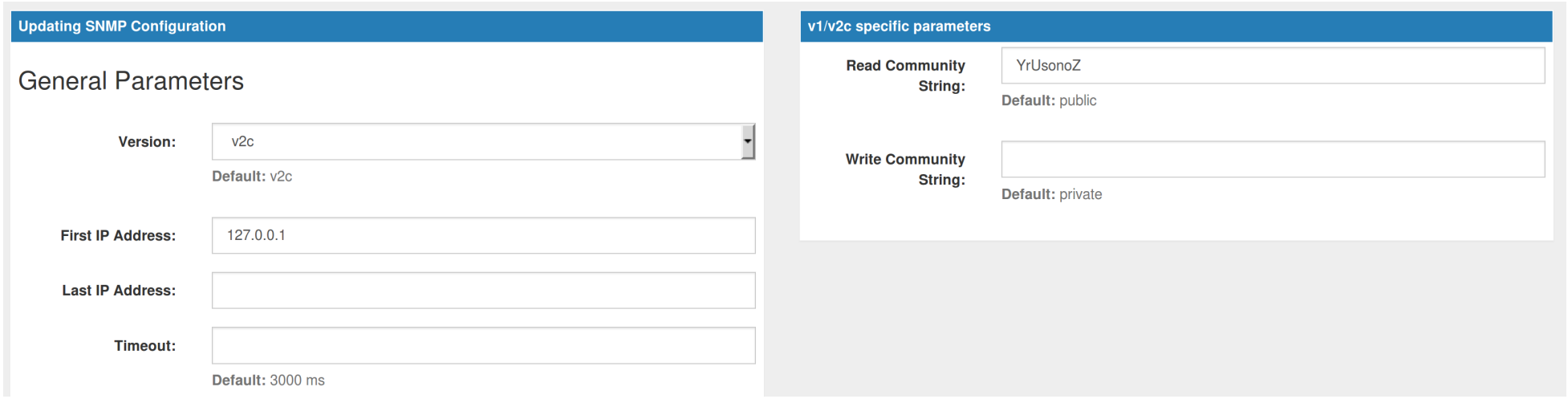
and look at the output.

Repeat the snmpwalk with “YrUsonoZ”:

```
snmpwalk -v2c -c YrUsonoZ localhost .1
```

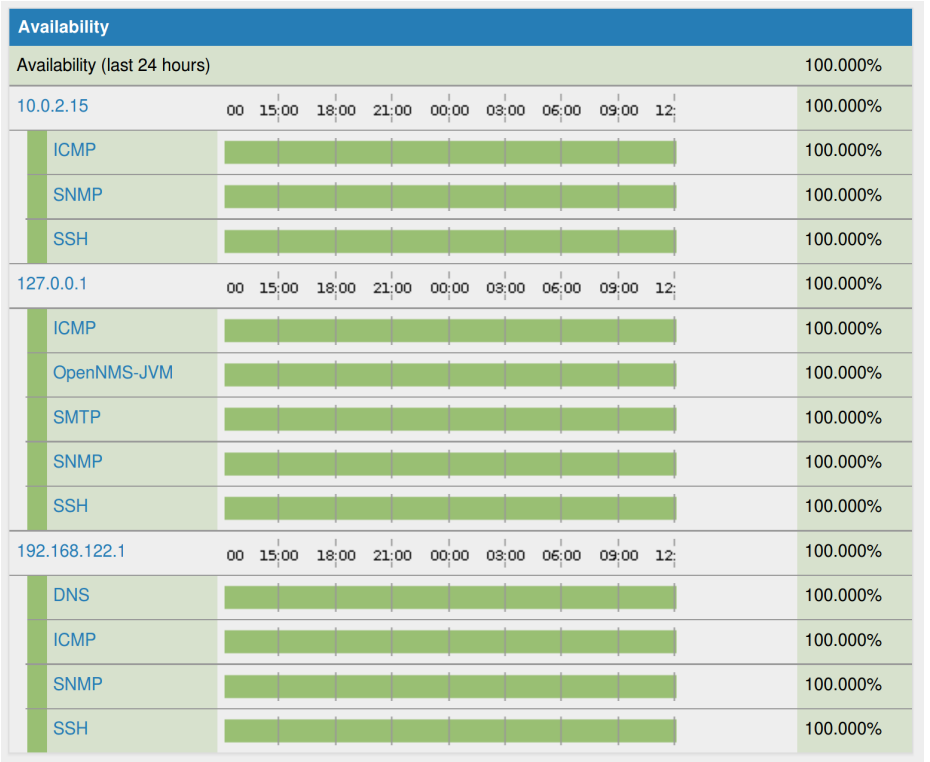
Set the Community String

Navigate to Configure → Configure SNMP Community Names by IP Address



Discover SNMP on localhost

Rescan the localhost node, note SNMP data and interfaces



snmp-config.xml

```
<snmp-config
   xmlns="http://xmlns.opennms.org/xsd/config/snmp"
   version="v2c"
   read-community="public"
   timeout="1800" retry="1">
   <definition read-community="YrUsonoZ">
      <specific>127.0.0.1</specific>
   </definition>
</snmp-config>
```