Getting Started with SNMP

Mike Weber

mweber@spidertools.com

Nagios® World Conference North America

The Library: Selecting a Book

- Library
- American History
- Civil War
- Ironclads
- Book:
  The Monitor and the Merrimack

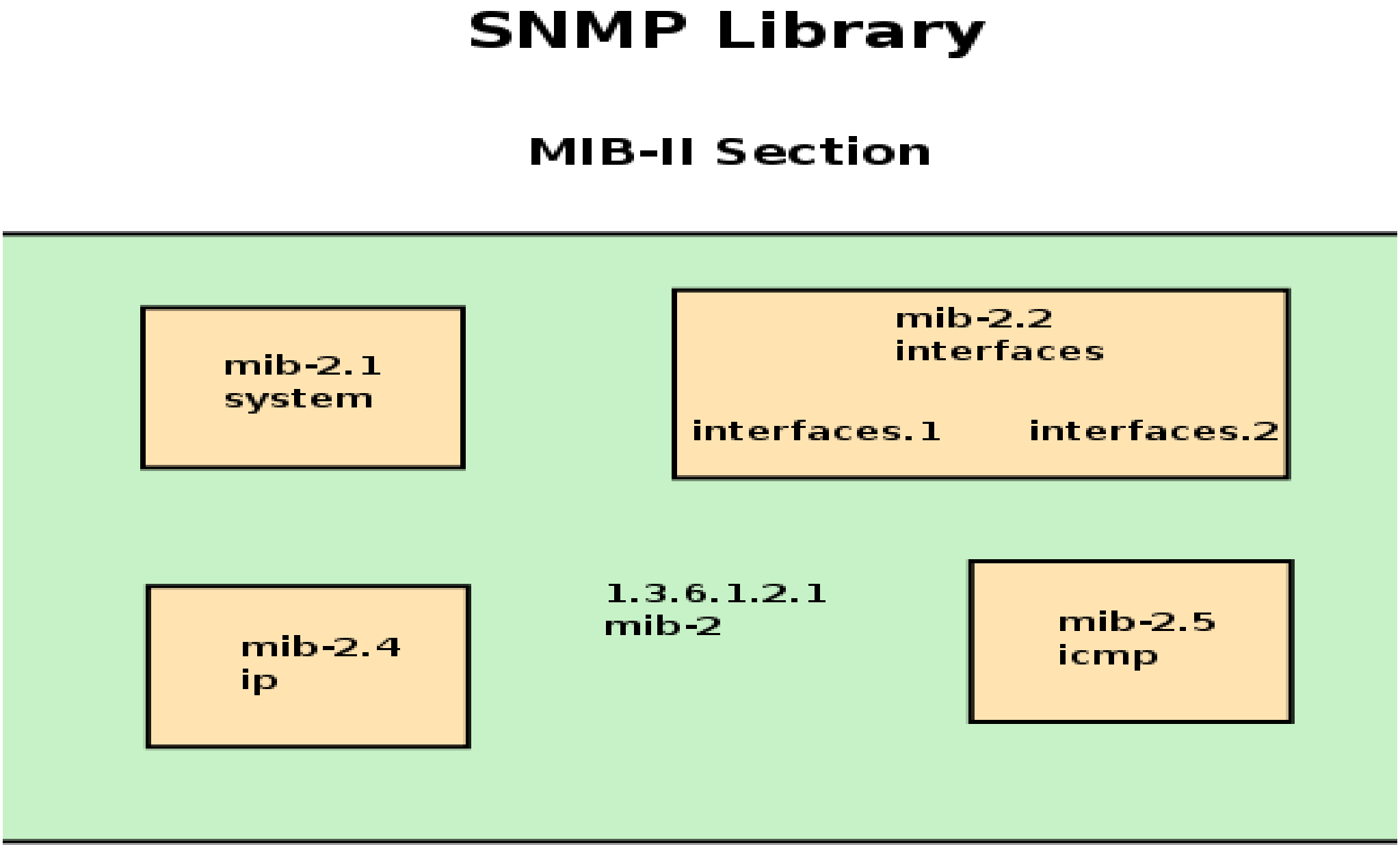
The SNMP Library: Selecting an OID

- SNMP Library
- American History
  1.3.6.1.2 mgmt
- Civil War
  1.3.6.1.2.1 mib-2
- Book / OID
  DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3422723) 9:30:27.23

SNMP Library Numbering: Hierarchical Tree

1 – iso
- 1.3 – org
  - 1.3.6 – dod
    - 1.3.6.1 – internet
      - 1.3.6.1.1 – directory
      - 1.3.6.1.2 – mgmt
        - 1.3.6.1.2.1 mib-2
      - 1.3.6.1.3 – experimental
      - 1.3.6.1.4 – private
      - 1.3.6.1.5 – security
      - 1.3.6.1.6 - SNMPv2

SNMP Library Sections: MIBs



SNMP Library Books: MIBs

Management Information Base

MIBS **provide a map** between numeric OIDs and a textual human readable format.

```
 snmpget -v2c -c public 172.16.37.1 ifDescr.2
IF-MIB::ifDescr.2 = STRING: eth0

 snmpget -v2c -c public -On 172.16.37.1 ifDescr.2
.1.3.6.1.2.1.2.2.1.2.2 = STRING: eth0
```

human readable	ifDescr.2
numeric	.1.3.6.1.2.1.2.2.1.2.2

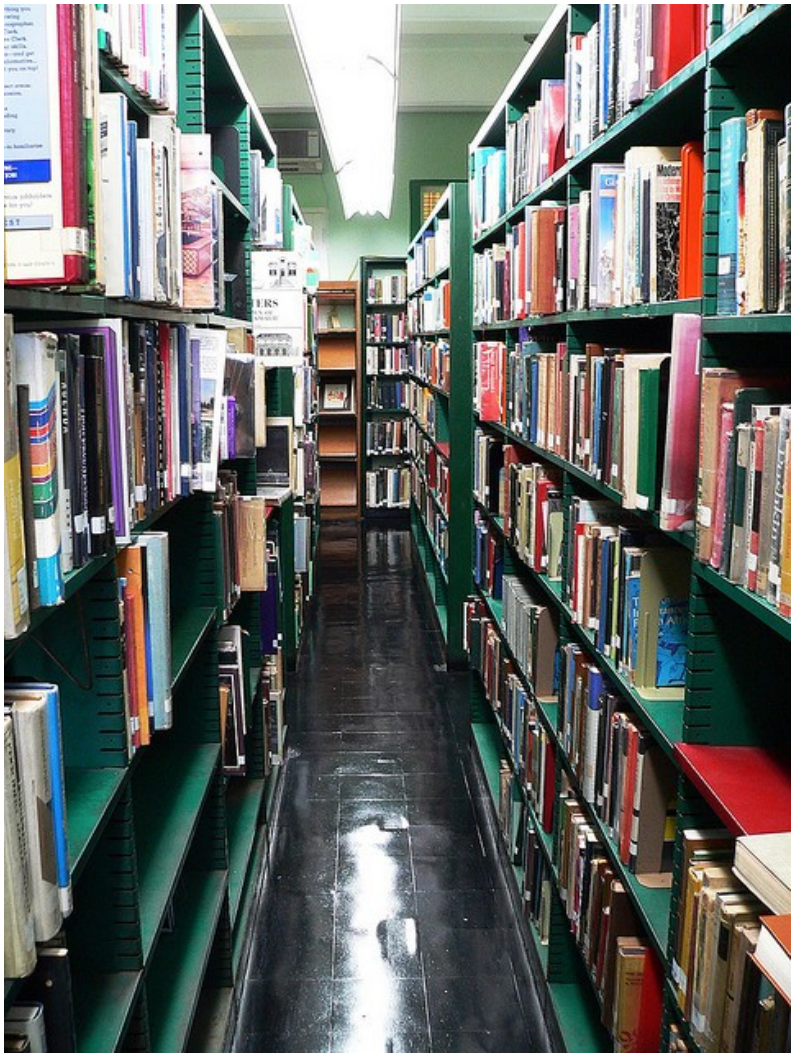
SNMP Library Books: MIBs

Management Information Base

MIBS **provide** a list of available OIDS, that is why in library sense it is a section.

```
IfEntry ::=
    SEQUENCE {
        ifIndex                 InterfaceIndex,
        ifDescr                 DisplayString,
        ifType                  IANAifType,
        ifMtu                   Integer32,
        ifSpeed                 Gauge32,
        ifPhysAddress           PhysAddress,
        ifAdminStatus           INTEGER,
        ifOperStatus            INTEGER,
        ifLastChange            TimeTicks,
        ifInOctets              Counter32,
        ifInUcastPkts           Counter32,
        ifInNUcastPkts          Counter32,  -- deprecated
        ifInDiscards            Counter32,
        ifInErrors              Counter32,
        ifInUnknownProtos       Counter32,
        ifOutOctets             Counter32,
        ifOutUcastPkts          Counter32,
        ifOutNUcastPkts         Counter32,  -- deprecated
        ifOutDiscards           Counter32,
        ifOutErrors             Counter32,
        ifOutQLen               Gauge32,    -- deprecated
        ifSpecific              OBJECT IDENTIFIER -- deprecated
```

SNMP Library Books: OIDs



Object Identifiers

OIDs are just like books, individual units of information that can be used to discover new information.

Here are some examples:
sysContact
sysDescr
ifDescr.2
sysUpTimeInstance

Each of these “books” represent a small part of a larger library.

SNMP Library Books: OIDs

Object Identifiers

An OID provides a unique key-value pair that is provided by the agent on the device. The agent populates the values to provide the “content” of the book.

Here are some examples:

```
sysContact.0 = STRING: root
sysDescr.0 = STRING: Linux db 2.6.32-5-686 #1 SMP Fri Sep 9 20:51:05 UTC 2011 i686
ifDescr.2 = STRING: eth0
sysUpTimeInstance = Timeticks: (3279) 0:00:32.79
```

Each of these “books” represent a small part of a larger library, the content or values are unique to the key on this device.

SNMP Library Tools

- Discovery Tools

  In any large library locating good tools and knowing how to use those tools are requirements for finding the books (OIDs) that you need.

- snmpwalk
- snmpget

SNMP Library Tools: Preparation

Gaining Permission on a Router

In order to use tools to search and monitor the router you must have permission to do so.

Cisco Router

config t
int e0
ip access-group 1 in
access-list 1 permit any
snmp-server community public RO

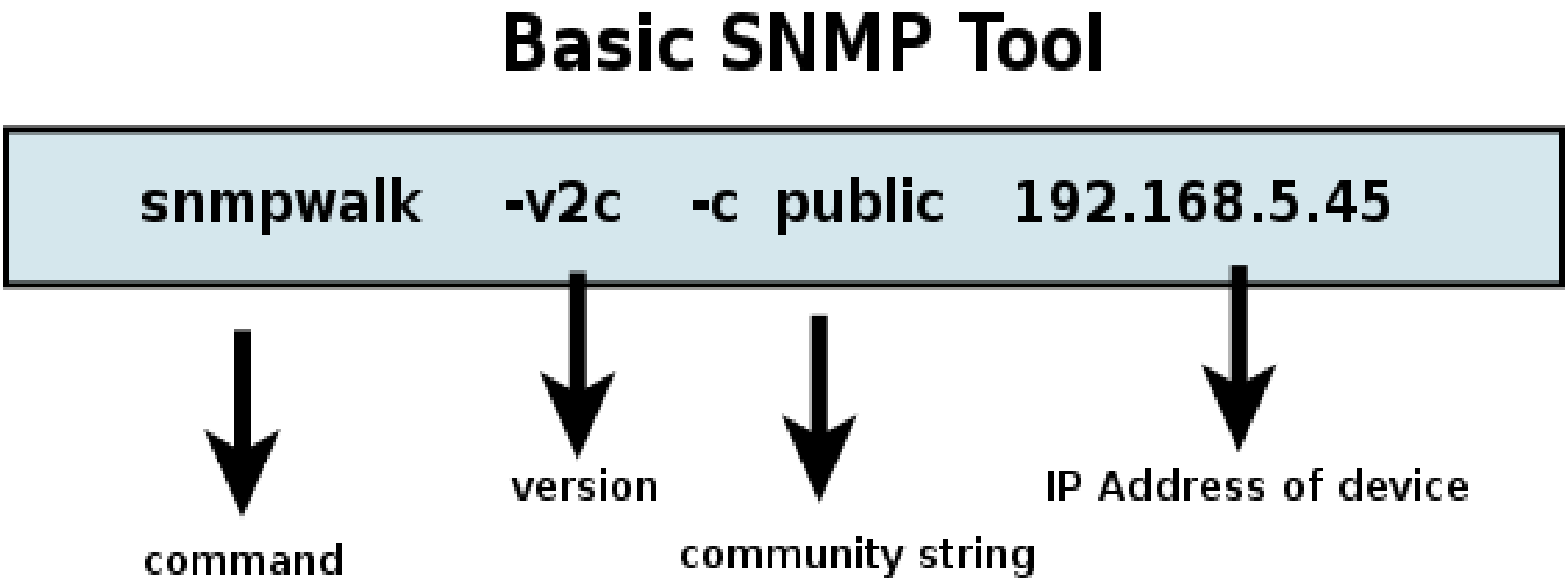
Router Settings

Those are simply basic settings so you can access the router using SNMP tools.

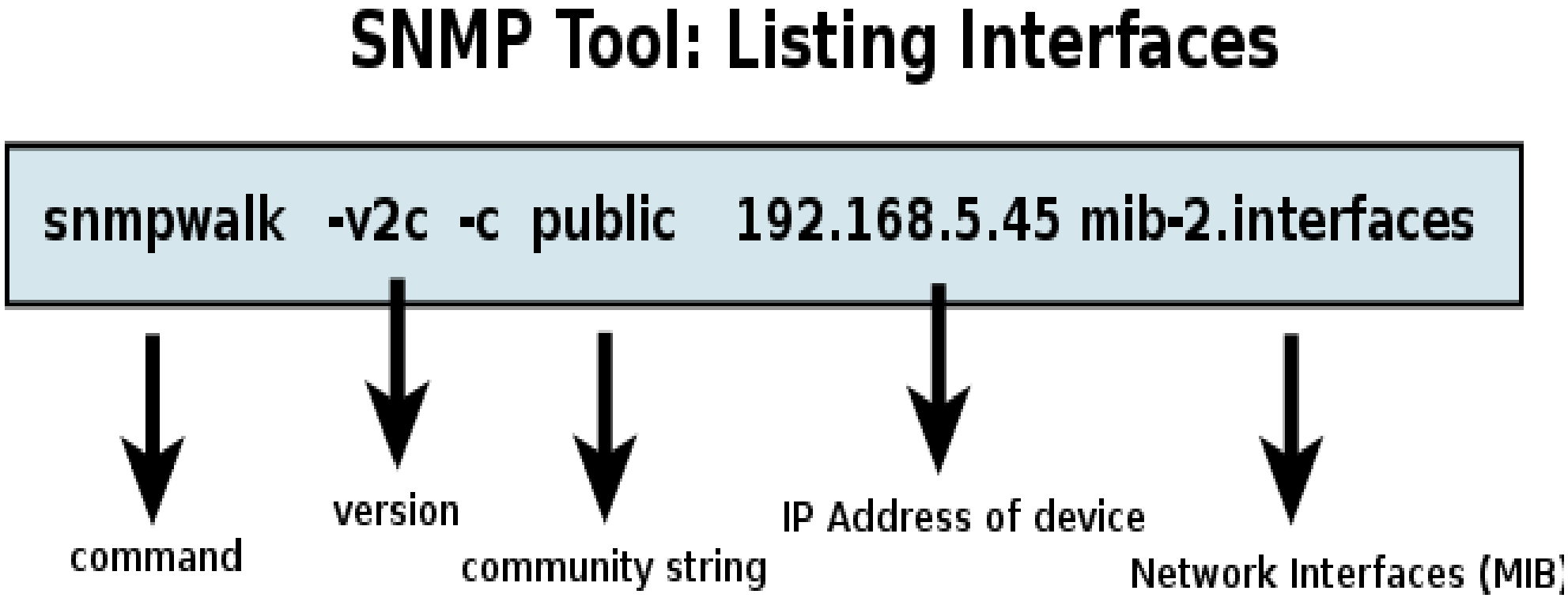
SNMP Library Tools: Preparation

- Gaining Permission on a Linux Server
  In order to use tools to search and monitor theserver you must have permission to do so.
- Install Net-SNMP on Server
  ```
  yum install -y net-snmp
  ```
- Linux Server
  ```
  com2sec notConfigUser   192.168.5.4  public
  group   notConfigGroup v1           notConfigUser
  group   notConfigGroup v2c           notConfigUser
  view     all    included  .1                               80
  access  notConfigGroup ""      any       noauth    exact  all
  none none
  ```
- Server Settings
  Those are simply basic settings so you can access the server using SNMP tools.

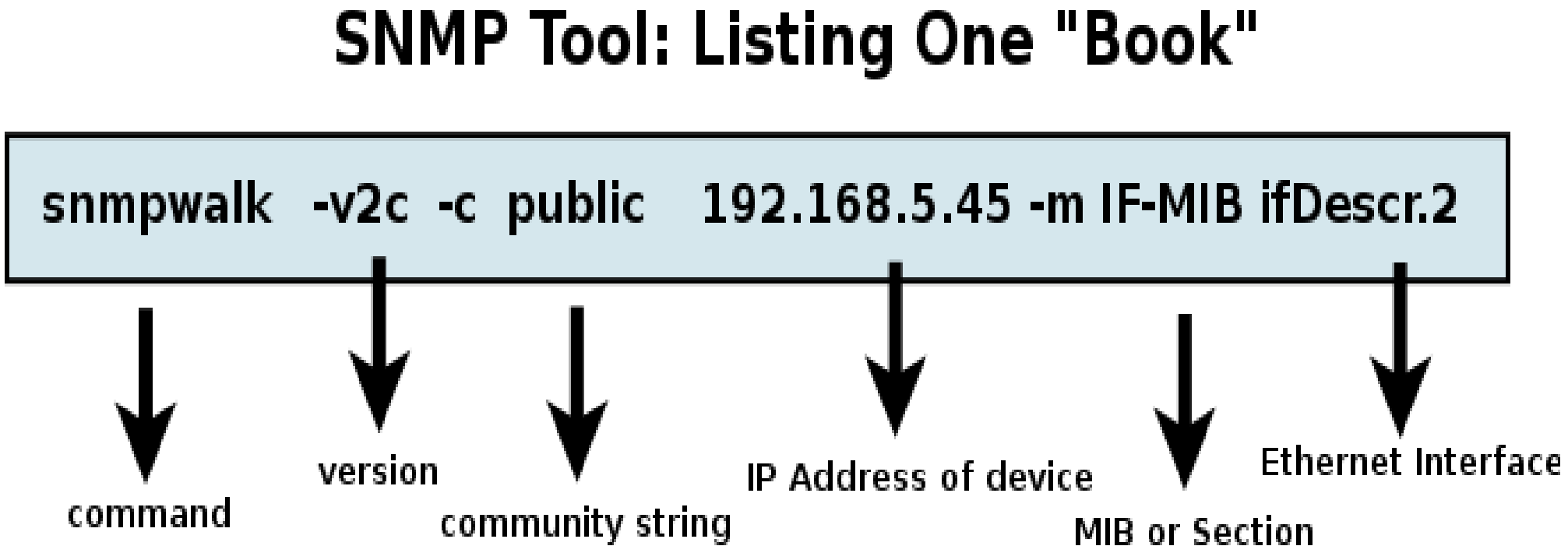
SNMP Library Tools: snmpwalk



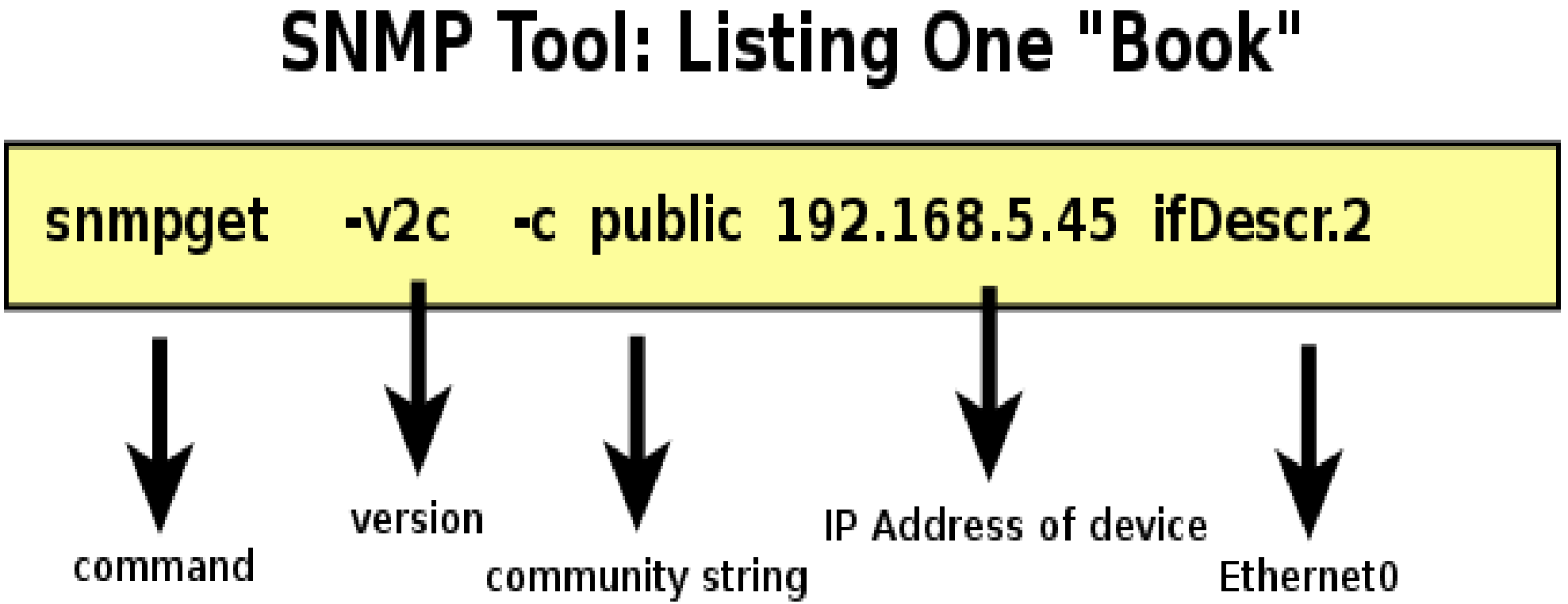
SNMP Library Tools: snmpwalk



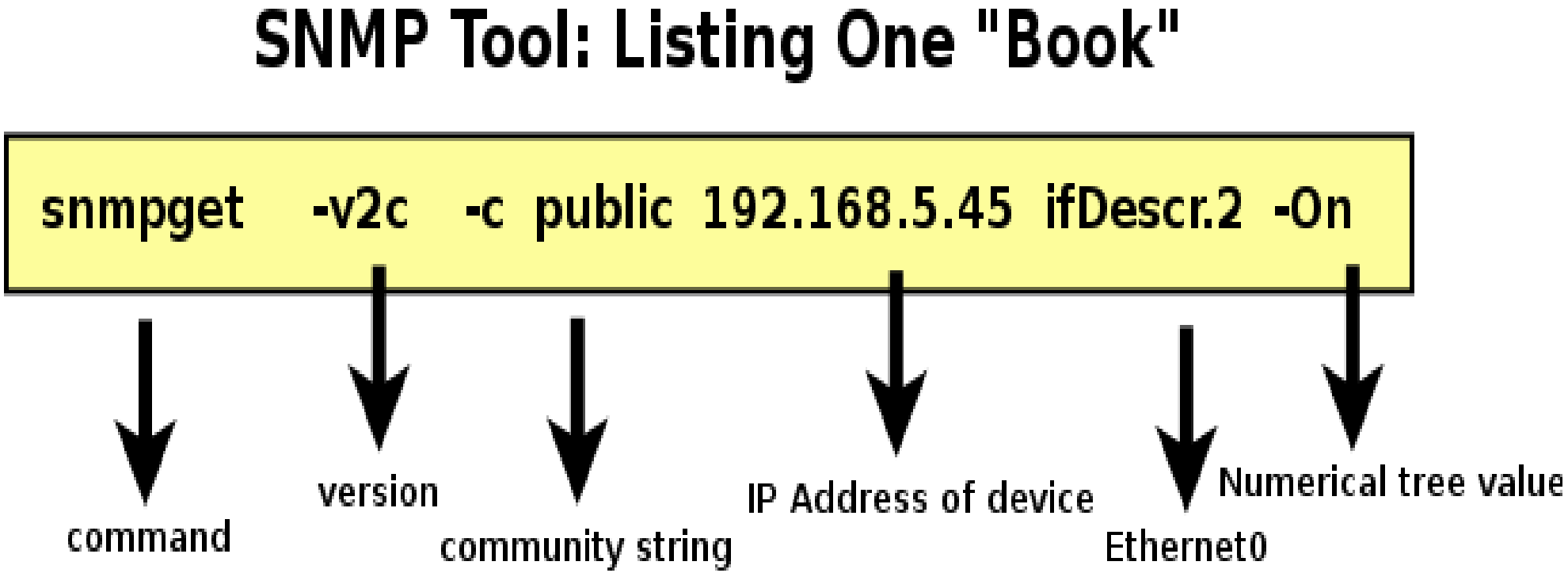
SNMP Library Tools: snmpwalk



SNMP Library Tools: snmpget



SNMP Library Tools: snmpget



SNMP Library: Creating a Reference

- Review the OIDs (books in the library)

```
snmpwalk -v2c -c public 172.16.37.1
SNMPv2-MIB::sysDescr.0 = STRING: Linux db 2.6.32-5-686 #1 SMP Fri Sep 9 20:51:05 UTC 2011 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3279) 0:00:32.79
SNMPv2-MIB::sysContact.0 = STRING: root
SNMPv2-MIB::sysName.0 = STRING: db
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
```

- Create a Database to Review

```
snmpwalk -v2c -c public 172.16.37.1 > snmp_host
```

SNMP Library: Creating a Reference

- Pick Out What You Know

```
vi snmp_host
SNMPv2-MIB::sysDescr.0 = STRING: Linux db 2.6.32-5-686 #1 SMP Fri Sep 9 20:51:05 UTC 2011 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3279) 0:00:32.79
SNMPv2-MIB::sysContact.0 = STRING: root
SNMPv2-MIB::sysName.0 = STRING: db
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifAdminStatus.4 = INTEGER: down(2)
IF-MIB::ifAdminStatus.5 = INTEGER: up(1)
IF-MIB::ifAdminStatus.6 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: down(2)
IF-MIB::ifOperStatus.3 = INTEGER: up(1)
IF-MIB::ifOperStatus.4 = INTEGER: down(2)
IF-MIB::ifOperStatus.5 = INTEGER: up(1)
IF-MIB::ifOperStatus.6 = INTEGER: up(1)
```

SNMP Library: Creating a Reference

- Create Searches in the Database

```
grep -i system snmp_host
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (47178) 0:07:51.78
HOST-RESOURCES-MIB::hrSystemDate.0 = STRING: 2011-9-24,5:58:28.0,-6:0
HOST-RESOURCES-MIB::hrSystemInitialLoadDevice.0 = INTEGER: 1536
HOST-RESOURCES-MIB::hrSystemInitialLoadParameters.0 = STRING: "BOOT_IMAGE=/vmlinuz-2.6.32-5-686 root=UUID=1ccd63f4-
a603-48be-8441-1f3859943ed5 ro quiet
```

```
grep -i Type snmp_host
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.6 = INTEGER: ethernetCsmacd(6)
```

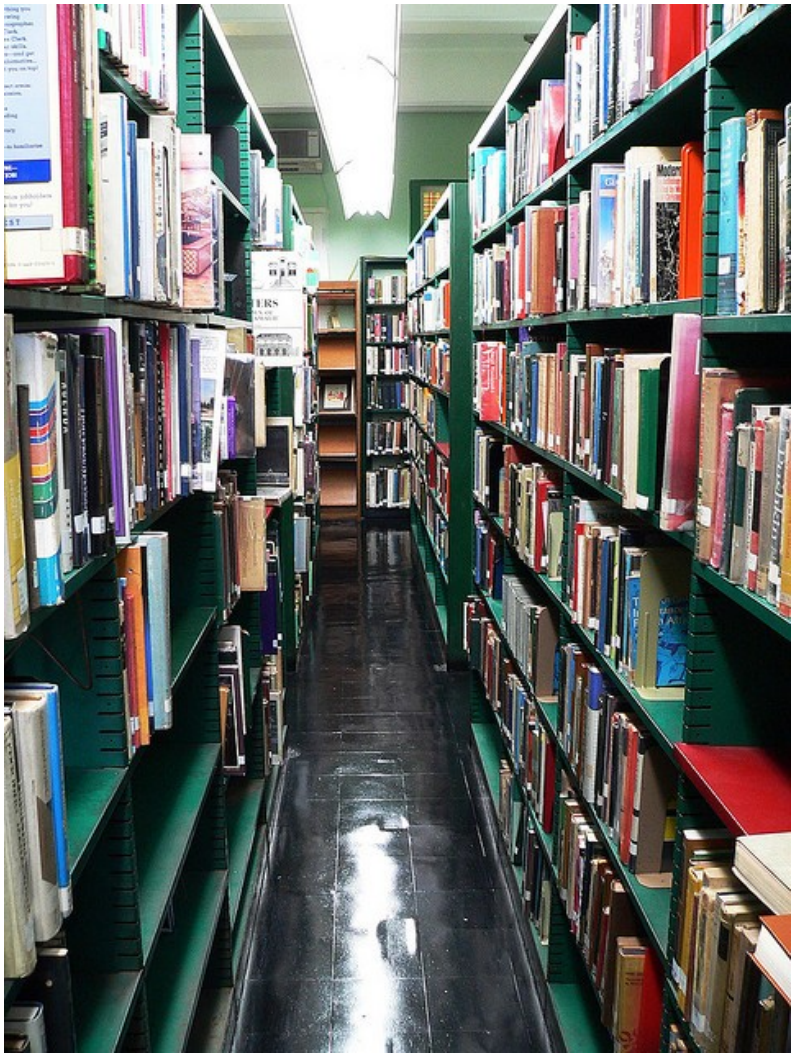
```
grep -i physical snmp_host
IP-MIB::ipNetToPhysicalPhysAddress.3.ipv4."192.168.5.103" = STRING: 0:1b:fc:68:68:33
IP-MIB::ipNetToPhysicalPhysAddress.3.ipv4."192.168.5.222" = STRING: e0:91:f5:7:1f:a5
IP-MIB::ipNetToPhysicalPhysAddress.6.ipv4."172.16.37.134" = STRING: 0:c:29:af:2e:b7
IP-MIB::ipNetToPhysicalType.3.ipv4."192.168.5.103" = INTEGER: dynamic(3)
IP-MIB::ipNetToPhysicalType.3.ipv4."192.168.5.222" = INTEGER: dynamic(3)
IP-MIB::ipNetToPhysicalType.6.ipv4."172.16.37.134" = INTEGER: dynamic(3)
IP-MIB::ipNetToPhysicalState.3.ipv4."192.168.5.103" = INTEGER: reachable(1)
IP-MIB::ipNetToPhysicalState.3.ipv4."192.168.5.222" = INTEGER: reachable(1)
IP-MIB::ipNetToPhysicalState.6.ipv4."172.16.37.134" = INTEGER: reachable(1)
IP-MIB::ipNetToPhysicalRowStatus.3.ipv4."192.168.5.103" = INTEGER: active(1)
IP-MIB::ipNetToPhysicalRowStatus.3.ipv4."192.168.5.222" = INTEGER: active(1)IP-
MIB::ipNetToPhysicalRowStatus.6.ipv4."172.16.37.134" = INTEGER: active(1)
```

SNMP Library: Creating a Reference

- Create Detailed Searches in the Database

```
grep -i hrSWRunName snmp_host
HOST-RESOURCES-MIB::hrSWRunName.1 = STRING: "init"
HOST-RESOURCES-MIB::hrSWRunName.2 = STRING: "kthreadd"
HOST-RESOURCES-MIB::hrSWRunName.3 = STRING: "migration/0"
HOST-RESOURCES-MIB::hrSWRunName.4 = STRING: "ksoftirqd/0"
HOST-RESOURCES-MIB::hrSWRunName.5 = STRING: "watchdog/0"
HOST-RESOURCES-MIB::hrSWRunName.6 = STRING: "migration/1"
HOST-RESOURCES-MIB::hrSWRunName.7 = STRING: "ksoftirqd/1"
HOST-RESOURCES-MIB::hrSWRunName.8 = STRING: "watchdog/1"
HOST-RESOURCES-MIB::hrSWRunName.9 = STRING: "events/0"
HOST-RESOURCES-MIB::hrSWRunName.10 = STRING: "events/1"
HOST-RESOURCES-MIB::hrSWRunName.11 = STRING: "cpuset"
HOST-RESOURCES-MIB::hrSWRunName.12 = STRING: "khelper"
HOST-RESOURCES-MIB::hrSWRunName.13 = STRING: "netns"
HOST-RESOURCES-MIB::hrSWRunName.14 = STRING: "async/mgr"
HOST-RESOURCES-MIB::hrSWRunName.15 = STRING: "pm"
HOST-RESOURCES-MIB::hrSWRunName.16 = STRING: "sync_supers"
HOST-RESOURCES-MIB::hrSWRunName.17 = STRING: "bdi-default"
HOST-RESOURCES-MIB::hrSWRunName.18 = STRING: "kintegrityd/0"
HOST-RESOURCES-MIB::hrSWRunName.19 = STRING: "kintegrityd/1"
```

SNMP Library



- You found a book now what?

Just like a book from the library, once you make the selection **you need to read the book** or use the information that you have located.

You have discovered that the OID ifDescr.2 refers to the Ethernet0 on the server. Now if you want to monitor that specific port, other options in the SNMP library tree will end in the "2" as well that refer to the Ethernet port.

SNMP Usage

Polling: Active Monitoring

Polling uses a command of script to make a request to the agent to typically to determine the values of a key. Here are several example of key-value pairs that may make up a request.

```
sysContact.0 = STRING: root
sysDescr.0 = STRING: Linux db 2.6.32-5-686 #1 SMP Fri Sep 9 20:51:05 UTC 2011 i686
ifDescr.2 = STRING: eth0
sysUpTimeInstance = Timeticks: (3279) 0:00:32.79
```

Traps: Passive Monitoring

The agent located on the device (think router, switch, server) contacts the *trap hos*t (think Nagios server) when an event occurs. Here are several examples.

```
LinkDown
LinkUp
authenticationFailure
```

SNMP Library: Testing the Plugin

- List the References to the Ethernet Port

```
IF-MIB::ifDescr.2 = STRING: Ethernet0
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifSpeed.2 = Gauge32: 10000000
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: up(1)
IF-MIB::ifLastChange.2 = Timeticks: (133639) 0:22:16.39
```

- Test check_snmp Plugin

```
./check_snmp -H 192.168.5.45 -C public -o ifAdminStatus.2

SNMP OK - 1 | IF-MIB::ifAdminStatus.2=1
```

SNMP Library: Create the Check

- Service Check

```
define service{
 use                             generic-service
 host_name                       db
 service_description             Ethernet Port
 check_command                   check_snmp!-C public -o ifAdminStatus.2
}
```

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
db	Ethernet Port	OK	09-07-2011 06:00:17	0d 0h 0m 41s	1/3	SNMP OK - 1
	GearUsers ?	WARNING	09-05-2011 13:26:04	1d 16h 34m 54s	1/3	USERS WARNING - 2 users currently logged in
	IMAP Port	OK	09-05-2011 12:50:04	2d 6h 32m 14s	1/3	TCP OK - 0.000 second response time on port 143
	POP3 Port	OK	09-05-2011 12:21:51	2d 6h 32m 7s	1/3	TCP OK - 0.000 second response time on port 110
	Postfix Port	OK	09-05-2011 12:00:17	2d 6h 32m 1s	1/3	TCP OK - 0.000 second response time on port 25
	SSH Port	OK	09-05-2011 11:35:21	2d 7h 16m 57s	1/3	TCP OK - 0.000 second response time on port 22
	Secure IMAPS	OK	09-05-2011 12:00:39	2d 6h 31m 39s	1/3	TCP OK - 0.000 second response time on port 993

SNMP Library: Create the Check on XI

Device Details

Device Address: 192.168.5.230

Host Name: 192.168.5.230

The name you'd like to have associated with this server or device.

SNMP Settings

Specify the settings used to monitor the server or device via SNMP.

SNMP Community: public

The SNMP community string required used to to query the device.

SNMP Version: 2c

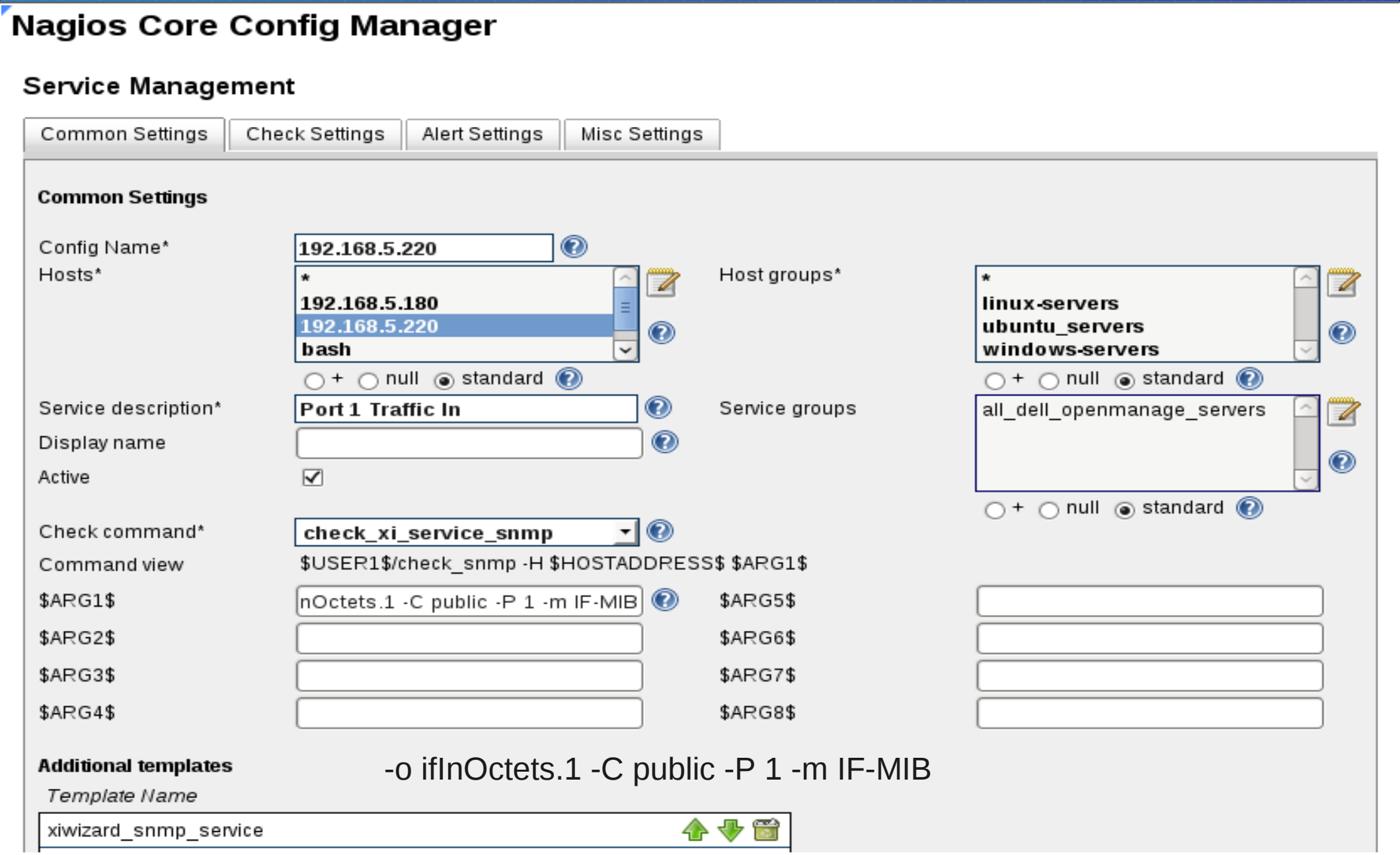
The SNMP protocol version used to commicate with the device.

SNMP Services

Specify any OIDs you'd like to monitor via SNMP. Sample entries have been provided as examples.

	OID	Display Name	Data Label	Data Units	Match Type	Warning Range	Critical Range	String To Match	MIB To Use
☐	sysUpTime.0	Uptime			None				
☐	ifOperStatus.1	Port 1 Status			String			1	RFC1213-MIB
☐	.1.3.6.1.4.1.2.3.51.1.2.1.5.1	IBM RSA II Adapter Tempera	Ambient Temp	Deg. Celsius	Numeric	29	35		
☐	1.3.6.1.4.1.3076.2.1.2.17.1.7	Cisco VPN Sessions	Active Sessions		Numeric	:70,:8	:75,:10		
☐					None				
☐					None				

SNMP Library: Create the Check on XI



-o ifInOctets.1 -C public -P 1 -m IF-MIB

SNMP Library: Create the Check on XI

Service Status

Host: **192.168.5.220**

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0

Unhandled	Problems	All
0	0	1

Last Updated: 2011-07-11 09:04:05

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
5	0	0	0	0

Unhandled	Problems	All
0	0	5

Last Updated: 2011-07-11 09:04:05

Showing 1-5 of 5 total records

Search... Go

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.220	Port 1 Last Change	Ok	26m 58s	1/5	2011-07-11 09:03:01	SNMP OK - Timeticks: (185065) 0:30:50.65
	Port 1 Status	Ok	25m 12s	1/5	2011-07-11 09:00:13	SNMP OK - up(1)
	Port 1 Traffic In	Ok	23m 41s	1/5	2011-07-11 09:01:48	SNMP OK - 171883
	SNMP Traps	Ok	36s	1/1	2011-07-11 09:03:59	A linkDown trap signifies that the SNMP entity, acting in 2 Serial0 propPointToPointSerial administratively down / ifIndex.2 (INTEGER32):2 ifDescr.2 (OCTETSTR):Serial0 ifType.2 (INTEGER):propPointToPointSerial enterprises.9.2.2.1.1.20.2 ():administrativel
	Uptime	Ok	26m 5s	1/5	2011-07-11 09:00:13	SNMP OK - Timeticks: (550048) 1:31:40.48

Page 1 of 1 15 Per Page Go

Last Updated: 2011-07-11 09:04:35