APNIC

SNMP Fundamentals

Table of Content

- What is SNMP (Simple Network Management Protocol)?
- SNMP Components
- SNMP Protocol Commands
- SNMP Version
- SNMP Communities
- SNMP – Packet Capture
- SNMP Configuration Examples

What is SNMP

- Simple Network Management Protocol
- Application layer protocol used to manage and monitor network devices and their functions
- What SNMP Does
  - Detect issues and fault early
  - Monitor device throughput
  - Remote configuration and control
- SNMP uses the User Datagram Protocol (UDP) as the transport protocol

RFC

rfc1157

SNMP Components

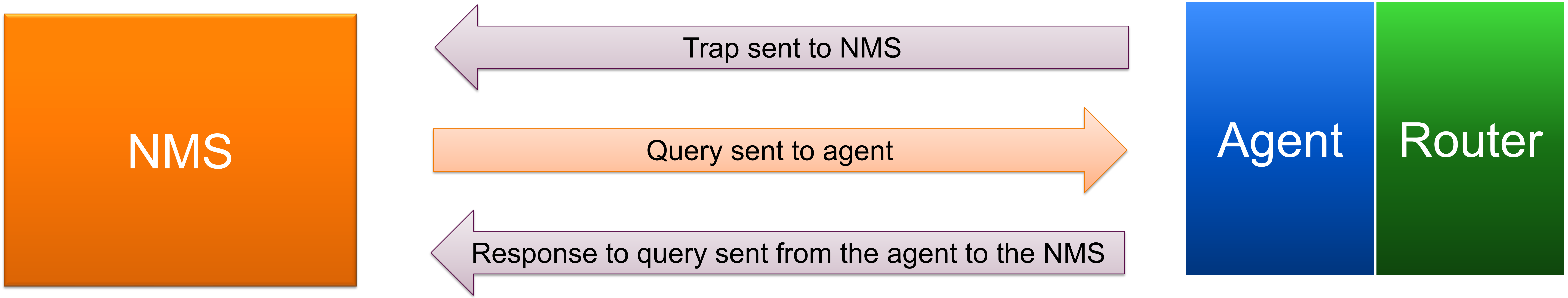
- SNMP Manager
- SNMP Agent
- Management Information Base (MIB)
- Managed Devices

SNMP Components – SNMP Manager

- SNMP Manager
  - Polls devices to obtain information and alerts
  - Typically a central software application
  - Option for email/SMS alerts to administrators
  - Poling happens over UDP port 161 (default)

SNMP Components – SNMP Agent

- SNMP Agent
  - Process running on a monitored device
  - Information sent as a response to poling
  - Unsolicited message (traps) can also be sent
  - Information sent over UDP port 162 (default)



Relationship between an NMS and an agent

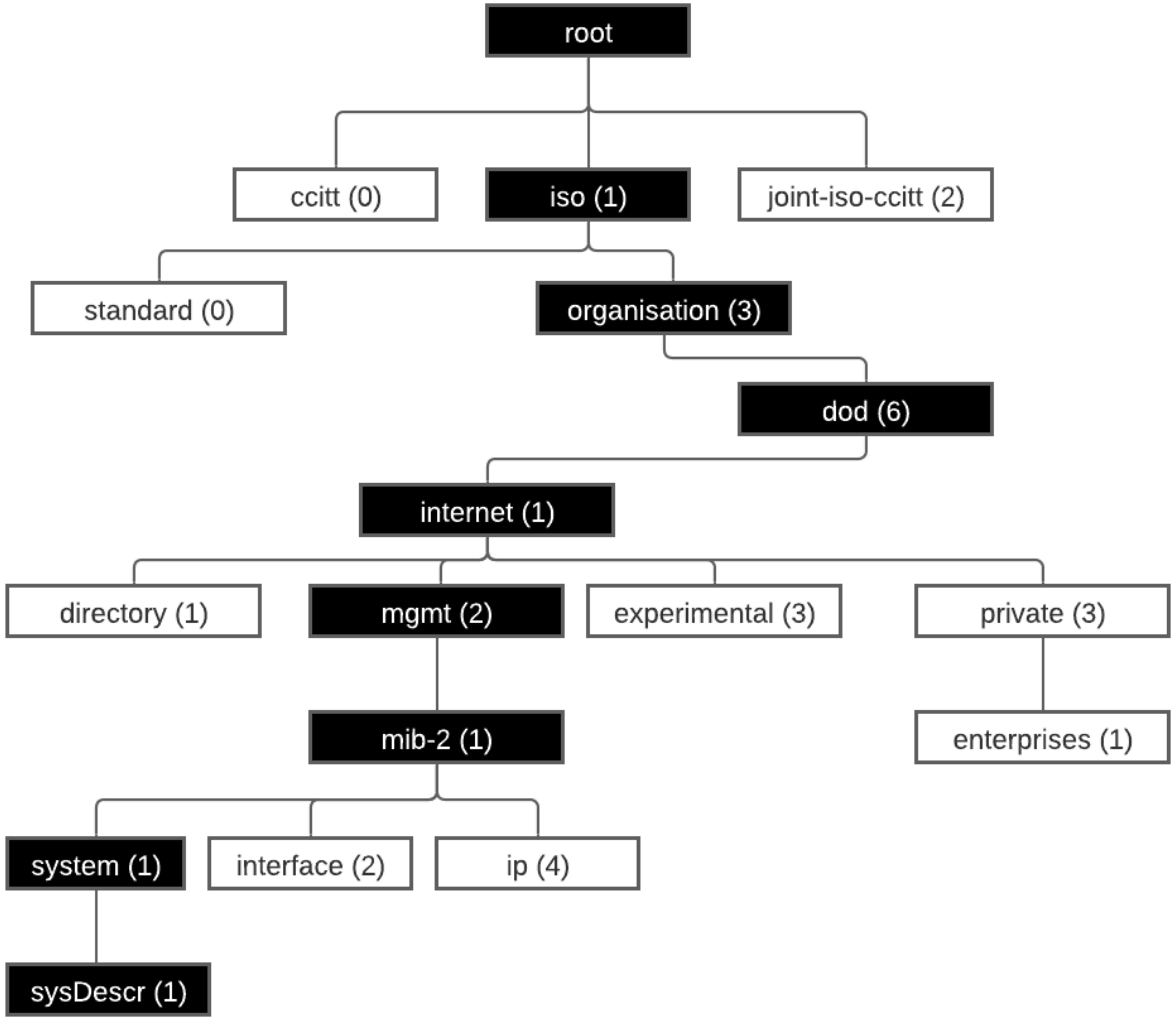
SNMP Components – MIB

- Management Information Base (MIB)
  - Collection of definitions which define the properties of the managed object
  - Each managed device keeps a database of values for each of the definitions written in the MIB
  - The MIB is a hierarchical structure that forms a tree and the MIB contains object identifiers or OIDs
  - An OID is an object identifier value, typically an address used to identify a particular device and its status

SNMP Components – OID in MIB

- SNMP-enabled network devices maintains database of system status, availability and performance information as objects, identified by OIDs

- For example, OID for system description (sysDescr) is **.1.3.6.1.2.1.1.1.0.** or **.iso.org.dod.internet.mgmt. mib-2.system.sysDescr.0**



SNMP Components – MIB

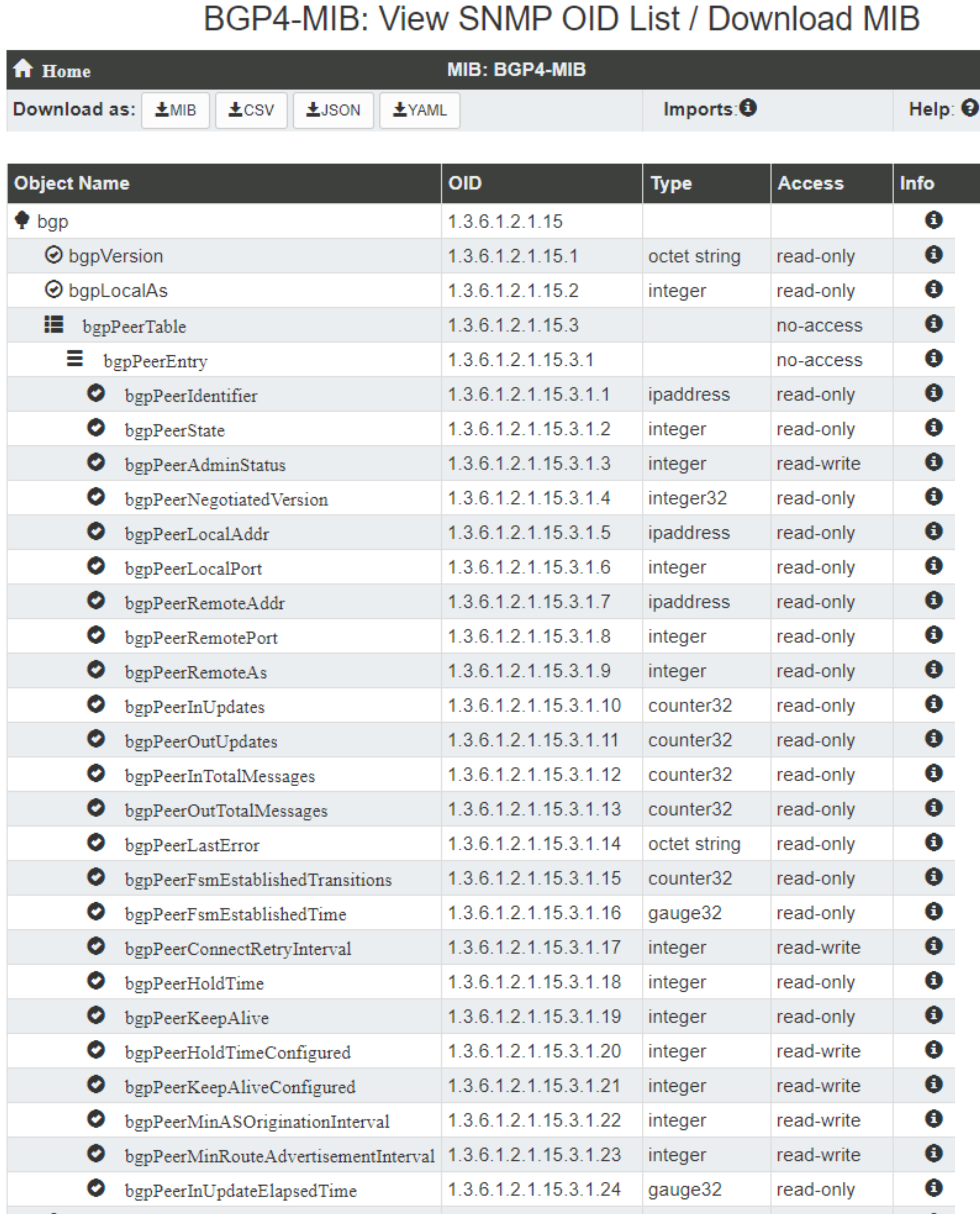
- An agent may implement many MIBs, but all agents implement a particular MIB called MIB-II
- The main goal of MIB-II (RFC 1213) is to provide general TCP/IP management information
  - interface speeds, MTU, octets sent, octets received, system location, system contact, etc
- There are many other draft and proposed standards
  - Interface Type MIB (RFC 2115)
  - BGP Version 4 MIB (RFC 1657)
  - DNS Server MIB (RFC 1611)
- Vendor also defines its own MIB (proprietary MIB)

RFC

rfc1213

SNMP Components – Standard MIB

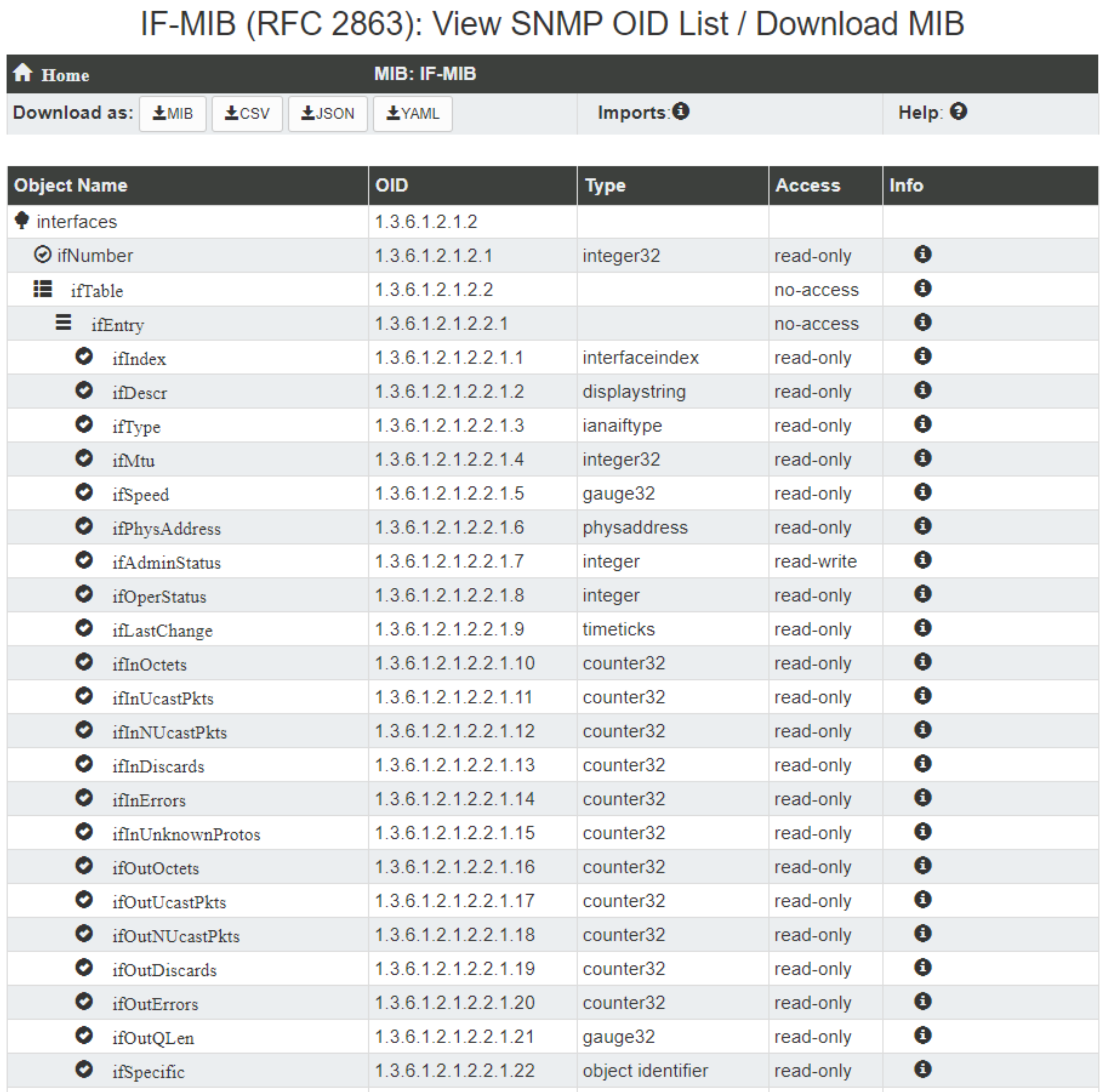
- Standard MIBs



BGP4-MIB: View SNMP OID List / Download MIB

Object Name	OID	Type	Access	Info
bgp	1.3.6.1.2.1.15			ℹ
bgpVersion	1.3.6.1.2.1.15.1	octet string	read-only	ℹ
bgpLocalAs	1.3.6.1.2.1.15.2	integer	read-only	ℹ
bgpPeerTable	1.3.6.1.2.1.15.3		no-access	ℹ
bgpPeerEntry	1.3.6.1.2.1.15.3.1		no-access	ℹ
bgpPeerIdentifier	1.3.6.1.2.1.15.3.1.1	ipaddress	read-only	ℹ
bgpPeerState	1.3.6.1.2.1.15.3.1.2	integer	read-only	ℹ
bgpPeerAdminStatus	1.3.6.1.2.1.15.3.1.3	integer	read-write	ℹ
bgpPeerNegotiatedVersion	1.3.6.1.2.1.15.3.1.4	integer32	read-only	ℹ
bgpPeerLocalAddr	1.3.6.1.2.1.15.3.1.5	ipaddress	read-only	ℹ
bgpPeerLocalPort	1.3.6.1.2.1.15.3.1.6	integer	read-only	ℹ
bgpPeerRemoteAddr	1.3.6.1.2.1.15.3.1.7	ipaddress	read-only	ℹ
bgpPeerRemotePort	1.3.6.1.2.1.15.3.1.8	integer	read-only	ℹ
bgpPeerRemoteAs	1.3.6.1.2.1.15.3.1.9	integer	read-only	ℹ
bgpPeerInUpdates	1.3.6.1.2.1.15.3.1.10	counter32	read-only	ℹ
bgpPeerOutUpdates	1.3.6.1.2.1.15.3.1.11	counter32	read-only	ℹ
bgpPeerInTotalMessages	1.3.6.1.2.1.15.3.1.12	counter32	read-only	ℹ
bgpPeerOutTotalMessages	1.3.6.1.2.1.15.3.1.13	counter32	read-only	ℹ
bgpPeerLastError	1.3.6.1.2.1.15.3.1.14	octet string	read-only	ℹ
bgpPeerFsmEstablishedTransitions	1.3.6.1.2.1.15.3.1.15	counter32	read-only	ℹ
bgpPeerFsmEstablishedTime	1.3.6.1.2.1.15.3.1.16	gauge32	read-only	ℹ
bgpPeerConnectRetryInterval	1.3.6.1.2.1.15.3.1.17	integer	read-write	ℹ
bgpPeerHoldTime	1.3.6.1.2.1.15.3.1.18	integer	read-only	ℹ
bgpPeerKeepAlive	1.3.6.1.2.1.15.3.1.19	integer	read-only	ℹ
bgpPeerHoldTimeConfigured	1.3.6.1.2.1.15.3.1.20	integer	read-write	ℹ
bgpPeerKeepAliveConfigured	1.3.6.1.2.1.15.3.1.21	integer	read-write	ℹ
bgpPeerMinASOriginationInterval	1.3.6.1.2.1.15.3.1.22	integer	read-write	ℹ
bgpPeerMinRouteAdvertisementInterval	1.3.6.1.2.1.15.3.1.23	integer	read-write	ℹ
bgpPeerInUpdateElapsedTime	1.3.6.1.2.1.15.3.1.24	gauge32	read-only	ℹ

https://bestmonitoringtools.com/mibdb/mibdb_search.php?mib=BGP4-MIB



IF-MIB (RFC 2863): View SNMP OID List / Download MIB

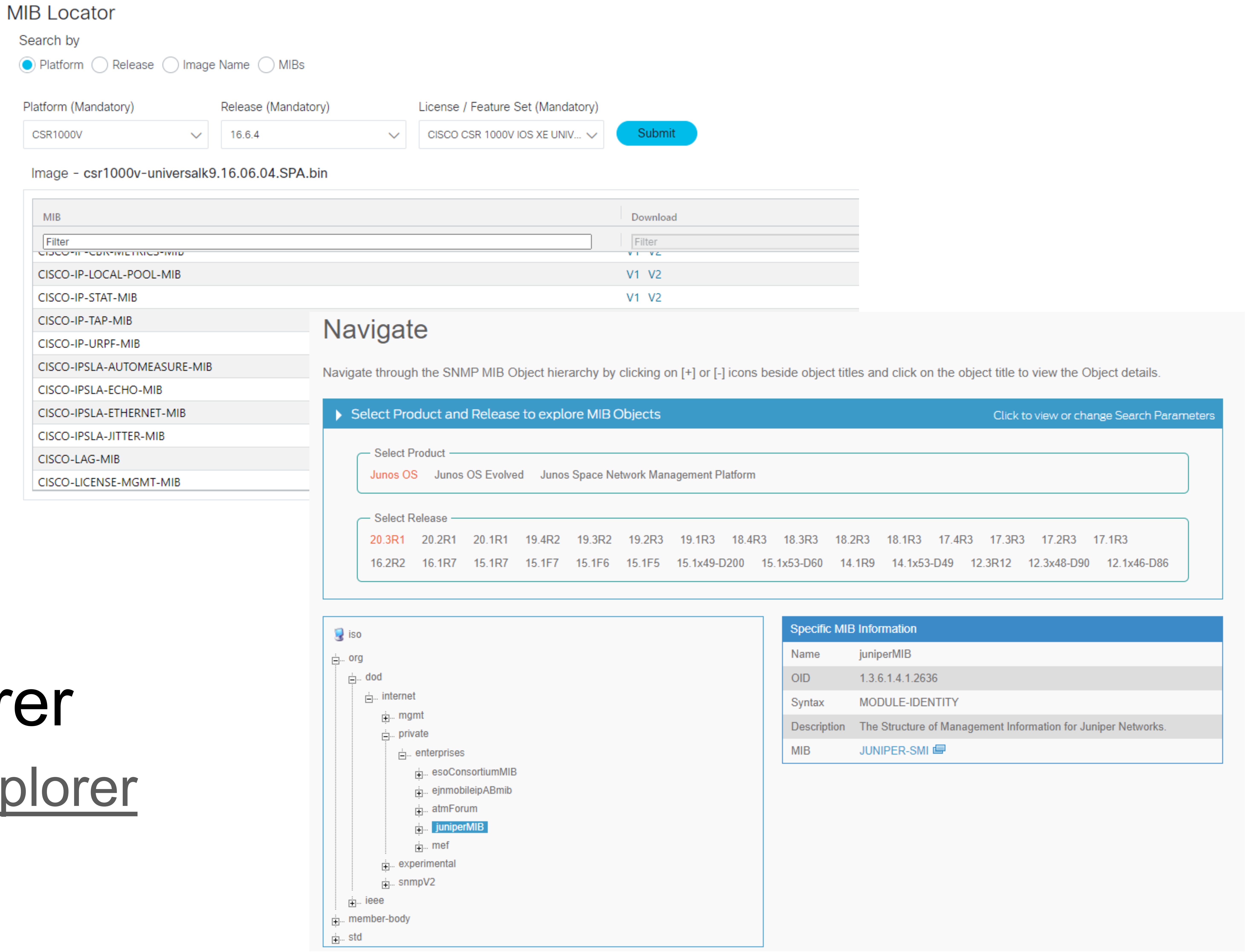
Object Name	OID	Type	Access	Info
interfaces	1.3.6.1.2.1.2			
ifNumber	1.3.6.1.2.1.2.1	integer32	read-only	ℹ
ifTable	1.3.6.1.2.1.2.2		no-access	ℹ
ifEntry	1.3.6.1.2.1.2.2.1		no-access	ℹ
ifIndex	1.3.6.1.2.1.2.2.1.1	interfaceindex	read-only	ℹ
ifDescr	1.3.6.1.2.1.2.2.1.2	displaystring	read-only	ℹ
ifType	1.3.6.1.2.1.2.2.1.3	ianaiftype	read-only	ℹ
ifMtu	1.3.6.1.2.1.2.2.1.4	integer32	read-only	ℹ
ifSpeed	1.3.6.1.2.1.2.2.1.5	gauge32	read-only	ℹ
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	physaddress	read-only	ℹ
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	integer	read-write	ℹ
ifOperStatus	1.3.6.1.2.1.2.2.1.8	integer	read-only	ℹ
ifLastChange	1.3.6.1.2.1.2.2.1.9	timeticks	read-only	ℹ
ifInOctets	1.3.6.1.2.1.2.2.1.10	counter32	read-only	ℹ
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	counter32	read-only	ℹ
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	counter32	read-only	ℹ
ifInDiscards	1.3.6.1.2.1.2.2.1.13	counter32	read-only	ℹ
ifInErrors	1.3.6.1.2.1.2.2.1.14	counter32	read-only	ℹ
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15	counter32	read-only	ℹ
ifOutOctets	1.3.6.1.2.1.2.2.1.16	counter32	read-only	ℹ
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	counter32	read-only	ℹ
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	counter32	read-only	ℹ
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	counter32	read-only	ℹ
ifOutErrors	1.3.6.1.2.1.2.2.1.20	counter32	read-only	ℹ
ifOutQLen	1.3.6.1.2.1.2.2.1.21	gauge32	read-only	ℹ
ifSpecific	1.3.6.1.2.1.2.2.1.22	object identifier	read-only	ℹ

https://bestmonitoringtools.com/mibdb/mibdb_search.php?mib=IF-MIB

SNMP Components – Proprietary MIB

- Cisco Feature Navigator
  - https://cfnng.cisco.com/mibs

- Juniper SNMP MIB Explorer
  - https://apps.juniper.net/mib-explorer



MIB Locator

Search by

● Platform ○ Release ○ Image Name ○ MIBs

Platform (Mandatory): CSR1000V

Release (Mandatory): 16.6.4

License / Feature Set (Mandatory): CISCO CSR 1000V IOS XE UNIV...

Image - csr1000v-universalk9.16.06.04.SPA.bin

MIB	Download
Filter	Filter
CISCO-IP-LOCAL-POOL-MIB	V1 V2
CISCO-IP-STAT-MIB	V1 V2
CISCO-IP-TAP-MIB	
CISCO-IP-URPF-MIB	
CISCO-IPSLA-AUTOMEASURE-MIB	
CISCO-IPSLA-ECHO-MIB	
CISCO-IPSLA-ETHERNET-MIB	
CISCO-IPSLA-JITTER-MIB	
CISCO-LAG-MIB	
CISCO-LICENSE-MGMT-MIB	

Navigate

Navigate through the SNMP MIB Object hierarchy by clicking on [+] or [-] icons beside object titles and click on the object title to view the Object details.

Select Product and Release to explore MIB Objects

Select Product: Junos OS | Junos OS Evolved | Junos Space Network Management Platform

Select Release: 20.3R1 20.2R1 20.1R1 19.4R2 19.3R2 19.2R3 19.1R3 18.4R3 18.3R3 18.2R3 18.1R3 17.4R3 17.3R3 17.2R3 17.1R3 16.2R2 16.1R7 15.1R7 15.1F7 15.1F6 15.1F5 15.1x49-D200 15.1x53-D60 14.1R9 14.1x53-D49 12.3R12 12.3x48-D90 12.1x46-D86

```
iso
⊟ org
    ⊟ dod
        ⊟ internet
            ⊞ mgmt
            ⊟ private
                ⊟ enterprises
                    ⊞ esoConsortiumMIB
                    ⊞ ejnmobileipABmib
                    ⊞ atmForum
                    ⊞ juniperMIB
                    ⊞ mef
            ⊞ experimental
            ⊞ snmpV2
    ⊞ ieee
⊞ member-body
⊞ std
```

Specific MIB Information

Name	juniperMIB
OID	1.3.6.1.4.1.2636
Syntax	MODULE-IDENTITY
Description	The Structure of Management Information for Juniper Networks.
MIB	JUNIPER-SMI

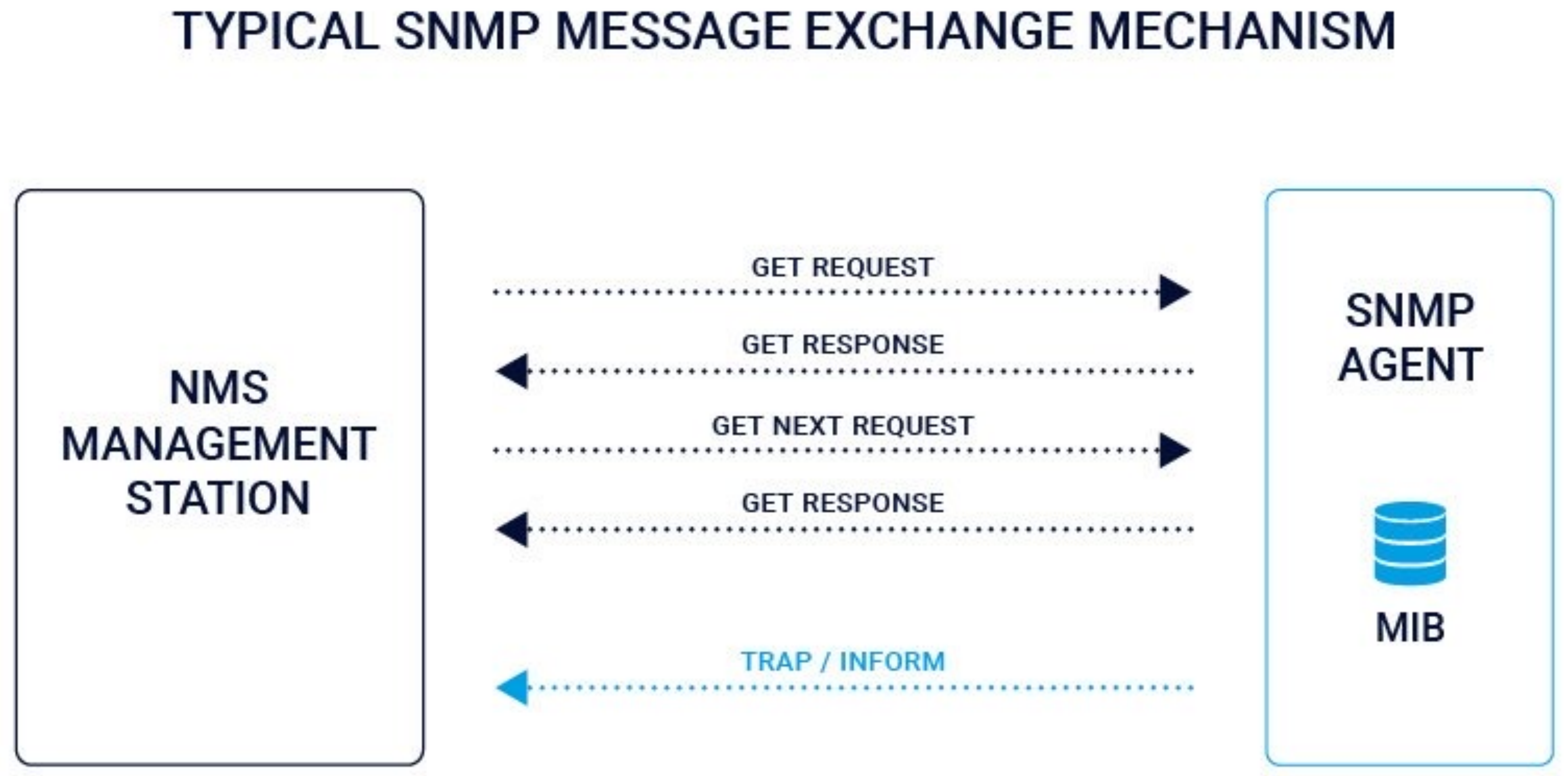
SNMP Components – Managed Devices

- Managed Devices
  - Controlled by an agent
  - SNMP information source

SNMP Protocol Commands

Messaging	Description
`Get`	A Get message is sent by a manager to an agent to request the value of a specific OID
`GetNext`	A GetNext message allows a manager to request the next sequential object in the MIB
`Set`	A Set message is sent by a manager to an agent in order to change the value held by a variable on the agent
`GetBulk`	This manager to agent request functions as if multiple GetNext requests were made
`Response`	This message, sent by an agent, is used to send any requested information back to the manager
`Trap`	Traps are asynchronous notifications in that they are unsolicited by the manager receiving them
`Inform`	Manager sends an Inform message back to the agent as acknowledgement

SNMP Message Exchange Mechanism



TYPICAL SNMP MESSAGE EXCHANGE MECHANISM

SNMP Version

- Three significant versions of SNMP
  - **SNMPv1**
    - Defined in RFC 1157
    - No inform-request option
    - Uses community string for security
    - Community string is passed in clear text
  - **SNMPv2**
    - Referred to as SNMP v2c
    - Addition of the inform-request option
    - Community string used for authentication
    - 64-bits counters
  - **SNMPv3**
    - Most current version
    - Addition of unique EngineIDs for SNMP devise
    - Adds authentication based on MD5 or SHA
    - Adds encryption through DES, 3DES or AES

SNMP Communities – SNMP v1 and v2

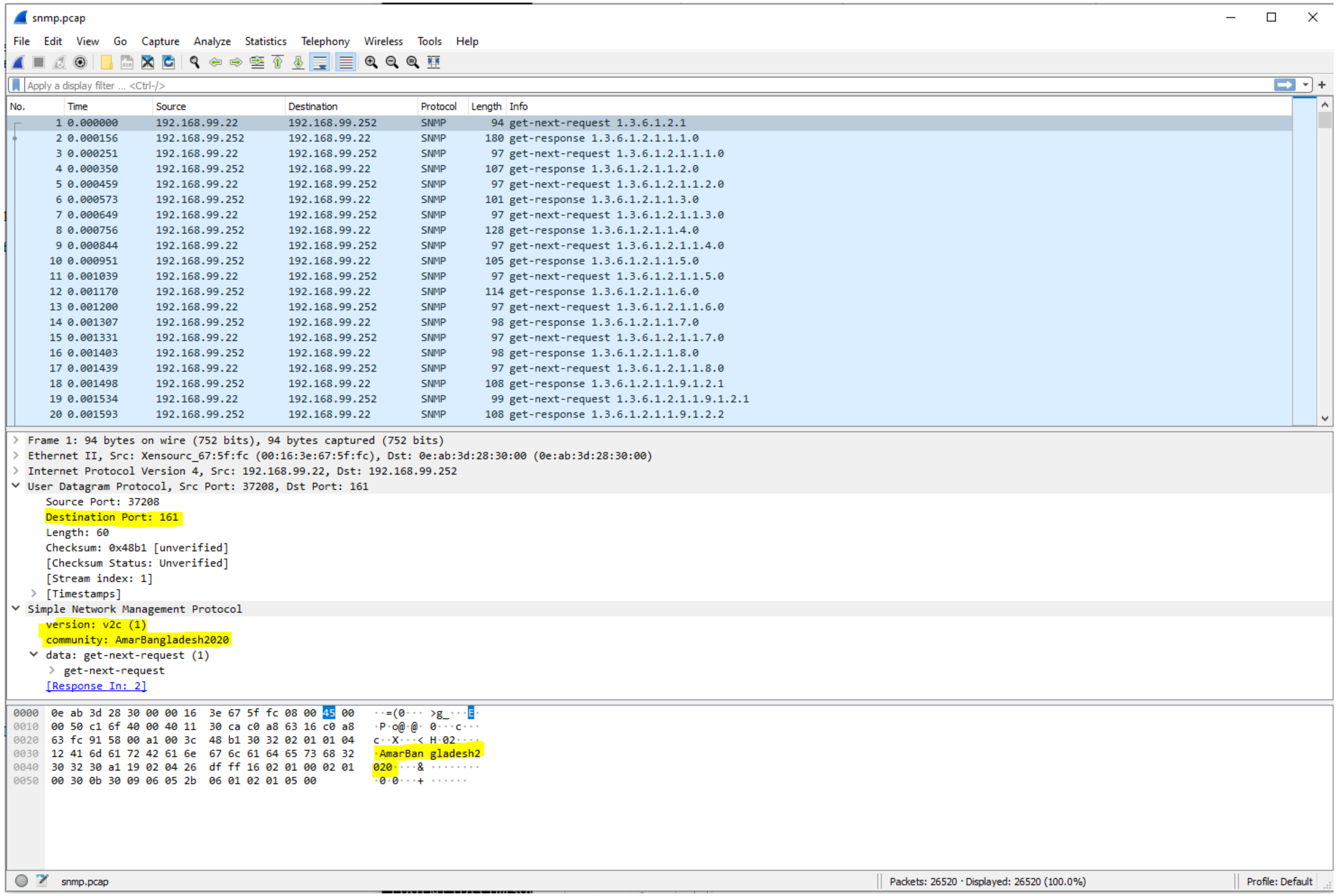
- SNMPv1 and SNMPv2 use communities to establish trust between managers and agents
- An agent is configured with three community names:
  - read-only
  - read-write and
  - trap
- The community names are essentially passwords
- Typically public for the read-only community and private for the read-write community

SNMPv3 Security Levels

- Ensure confidentiality, authentication and access control

	Authentication	Encryption	Username	Password
NoAuthNoPriv	No	No	Yes	No
AuthNoPriv	Yes	No	Yes	Yes
AuthPriv	Yes	Yes	Yes	Yes

SNMP – Packet Capture



snmp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.99.22   192.168.99.252  SNMP      94 get-next-request 1.3.6.1.2.1
   2 0.000156  192.168.99.252  192.168.99.22   SNMP     180 get-response 1.3.6.1.2.1.1.1.0
   3 0.000251  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.1.0
   4 0.000350  192.168.99.252  192.168.99.22   SNMP     107 get-response 1.3.6.1.2.1.1.2.0
   5 0.000459  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.2.0
   6 0.000573  192.168.99.252  192.168.99.22   SNMP     101 get-response 1.3.6.1.2.1.1.3.0
   7 0.000649  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.3.0
   8 0.000756  192.168.99.252  192.168.99.22   SNMP     128 get-response 1.3.6.1.2.1.1.4.0
   9 0.000844  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.4.0
  10 0.000951  192.168.99.252  192.168.99.22   SNMP     105 get-response 1.3.6.1.2.1.1.5.0
  11 0.001039  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.5.0
  12 0.001170  192.168.99.252  192.168.99.22   SNMP     114 get-response 1.3.6.1.2.1.1.6.0
  13 0.001200  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.6.0
  14 0.001307  192.168.99.252  192.168.99.22   SNMP      98 get-response 1.3.6.1.2.1.1.7.0
  15 0.001331  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.7.0
  16 0.001403  192.168.99.252  192.168.99.22   SNMP      98 get-response 1.3.6.1.2.1.1.8.0
  17 0.001439  192.168.99.22   192.168.99.252  SNMP      97 get-next-request 1.3.6.1.2.1.1.8.0
  18 0.001498  192.168.99.252  192.168.99.22   SNMP     108 get-response 1.3.6.1.2.1.1.9.1.2.1
  19 0.001534  192.168.99.22   192.168.99.252  SNMP      99 get-next-request 1.3.6.1.2.1.1.9.1.2.1
  20 0.001593  192.168.99.252  192.168.99.22   SNMP     108 get-response 1.3.6.1.2.1.1.9.1.2.2
```

```
> Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Ethernet II, Src: Xensourc_67:5f:fc (00:16:3e:67:5f:fc), Dst: 0e:ab:3d:28:30:00 (0e:ab:3d:28:30:00)
> Internet Protocol Version 4, Src: 192.168.99.22, Dst: 192.168.99.252
v User Datagram Protocol, Src Port: 37208, Dst Port: 161
    Source Port: 37208
    Destination Port: 161
    Length: 60
    Checksum: 0x48b1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
v Simple Network Management Protocol
    version: v2c (1)
    community: AmarBangladesh2020
  v data: get-next-request (1)
    > get-next-request
    [Response In: 2]
```

```
0000  0e ab 3d 28 30 00 00 16  3e 67 5f fc 08 00 45 00   ··=(0··· >g_···E·
0010  00 50 c1 6f 40 00 40 11  30 ca c0 a8 63 16 c0 a8   ·P·o@·@· 0···c···
0020  63 fc 91 58 00 a1 00 3c  48 b1 30 32 02 01 01 04   c··X···< H·02····
0030  12 41 6d 61 72 42 61 6e  67 6c 61 64 65 73 68 32   ·AmarBan gladesh2
0040  30 32 30 a1 19 02 04 26  df ff 16 02 01 00 02 01   020····& ········
0050  00 30 0b 30 09 06 05 2b  06 01 02 01 05 00         ·0·0···+ ······
```

snmpwalk -v 2c -c {community} 192.168.99.252

Configuration Example – SNMPv1 and v2

- Create a community with write access

```
router(config)# access-list 66 permit 192.168.11.5
router(config)# snmp-server community example1rw rw 66
```

- Create a community with read-only access

```
router(config)# access-list 67 permit 192.168.16.1
router(config)# snmp-server community example2ro ro 67
```

Configuration Example – SNMPv3

- Create a community with write access

```
router(config)# snmp-server view viewAPNIC iso included
router(config)# snmp-server group grpAPNIC v3 priv read viewAPNIC
router(config)# snmp-server user apnic grpAPNIC v3 auth sha AUTHPASS priv aes 128 PRIVPASS
```

SNMP Fundamentals

Module 2: LibreNMS

LibreNMS

- A Fully Featured Network Monitoring Tool for Linux
- LibreNMS is an open source, powerful and feature-rich auto-discovering PHP based network monitoring system which uses the SNMP protocol
- It supports a broad range of operating systems including Linux, FreeBSD, as well as network devices including Cisco, Juniper, Brocade, Foundry, HP and many more

LibreNMS - Features

- Some major features of LibreNMS
  - It auto-discovers a whole network using these protocols: CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP
  - Supports a Unix agent
  - Supports horizontal scaling to expand with your network
  - Supports a highly flexible and customizable alerting system; sends notifications through email, irc, slack and more
  - Supports an API for managing, graphing and retrieving data from your system
  - Offers a traffic billing system
  - Supports integration with NfSen, collectd, SmokePing, RANCID and Oxidized
  - Supports multiple authentication methods such as MySQL, HTTP, LDAP, Radius and Active Directory

LibreNMS vs Observium

- LibreNMS is a fork of Observium
- How LibreNMS will be different from Observium:
  - Inclusive community, where it's OK to ask stupid questions, and OK to ask for things that aren't on the roadmap.
  - Development decisions will be community-driven. Want to make software that fulfils its users' needs
  - There are no plans for a paid version
  - There are no current plans for paid support, but this may be added later if there is sufficient demand

LibreNMS - Architecture

- LibreNMS has following components:
  - **Web/API Layer**: This is typically Apache but we have setup guides for both Nginx and Lighttpd
  - **RRD (Time Series Data store)**: Central storage should be provided so all RRD files can be read from and written to in one location
  - **Database**: MySQL / MariaDB
  - **Poller/Discovery**: To gather information and discover network. Cron based polling is the common setup
- All these components may only be installed on one server
- For scaling LibreNMS; distributed polling has been used.

LibreNMS - Metrics

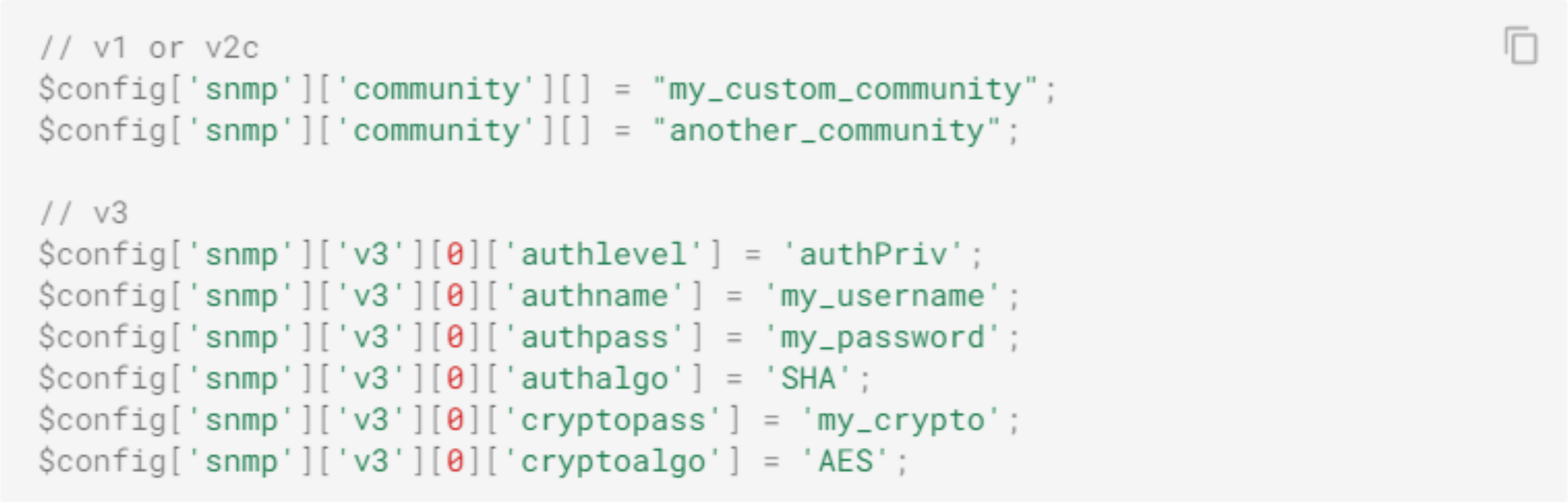
- LibreNMS supports wide range of metrics which includes:
  - Memory, Processor and Storage
  - Temperature, Voltage and Fan speed
  - Interface traffic and statistics
  - OS/Distribution detection
  - Routing information (BGP and OSPF)
  - Wide range of application monitoring (Apache, Asterisk, BIND, FreeRADIUS, MySQL, NTP, NGINX, Postfix, Squid, Unbound etc.)
    - https://docs.librenms.org/Extensions/Applications/
  - IPv4, IPv6, TCP and UDP statistics

LibreNMS - Metric Storage

- By default we ship all metrics to RRD files, either directly or via RRDCached
- On top of this we can ship metrics to
  - Graphite
  - InfluxDB
  - OpenTSDB
  - Prometheus
- At present these backends can’t be used to display graphs within LibreNMS and need to use something like Grafana

LibreNMS - Auto Discovery

- LibreNMS is based on SNMP
- Support following methods for auto discovery:
  - ARP
  - XDP (FDP, CDP, LLDP)
  - OSPF
  - BGP
  - SNMP Scan



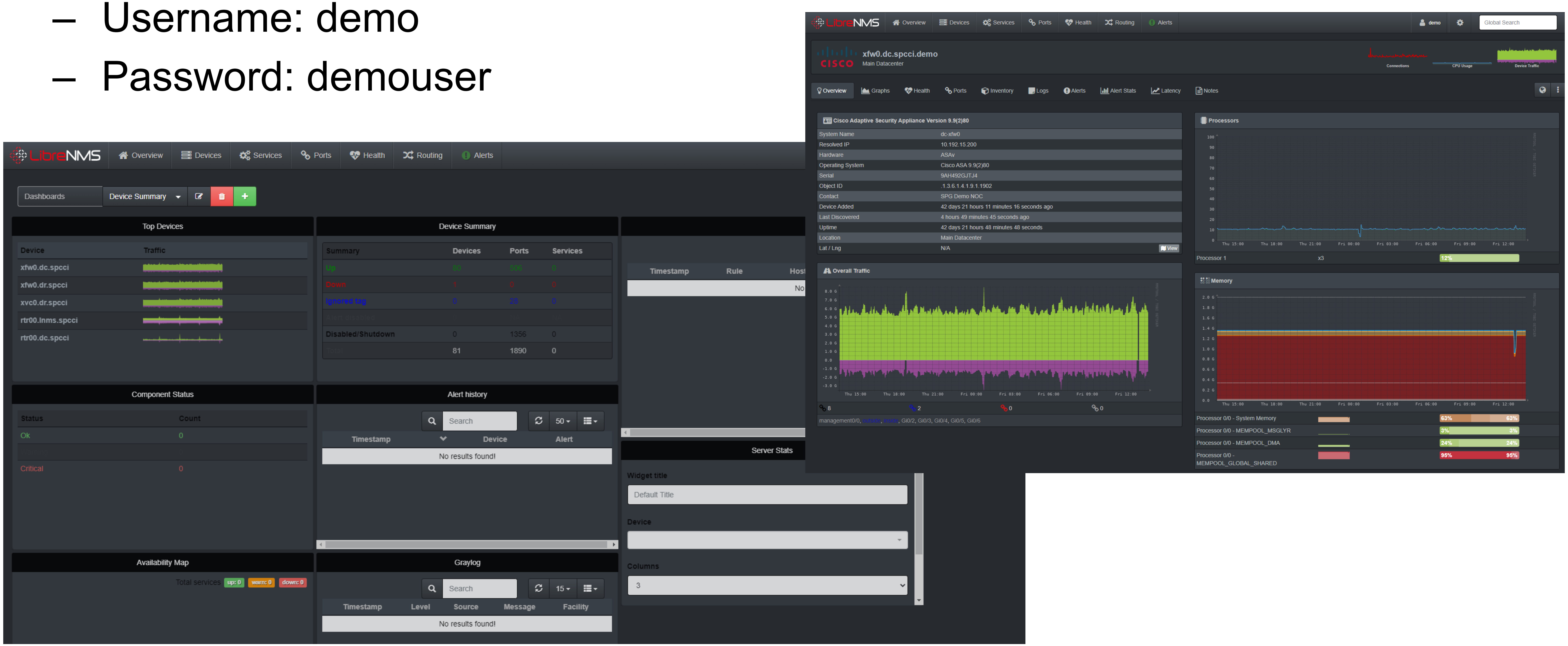
```
// v1 or v2c
$config['snmp']['community'][] = "my_custom_community";
$config['snmp']['community'][] = "another_community";

// v3
$config['snmp']['v3'][0]['authlevel'] = 'authPriv';
$config['snmp']['v3'][0]['authname'] = 'my_username';
$config['snmp']['v3'][0]['authpass'] = 'my_password';
$config['snmp']['v3'][0]['authalgo'] = 'SHA';
$config['snmp']['v3'][0]['cryptopass'] = 'my_crypto';
$config['snmp']['v3'][0]['cryptoalgo'] = 'AES';
```

LibreNMS - 3rd Party Integration

- LibreNMS integration
  - Graylog -> https://docs.librenms.org/Extensions/Graylog/
  - Nagios -> https://docs.librenms.org/Extensions/Services/
  - NFSen -> https://docs.librenms.org/Extensions/NFSen/
  - Oxdizied -> https://docs.librenms.org/Extensions/Oxidized/
  - Smokeping -> https://docs.librenms.org/Extensions/Smokeping/

LibreNMS - Demo

- Demo URL: https://demo.librenms.org/
  - Username: demo
  - Password: demouser



Device Summary

Summary	Devices	Ports	Services
Up	80	506	0
Down	1	0	0
Ignored tag	0	28	0
Alert disabled	0	NA	NA
Disabled/Shutdown	0	1356	0
Total	81	1890	0

Cisco Adaptive Security Appliance Version 9.9(2)80

System Name	dc-xfw0
Resolved IP	10.192.15.200
Hardware	ASAv
Operating System	Cisco ASA 9.9(2)80
Serial	9AH492GJTJ4
Object ID	.1.3.6.1.4.1.9.1.1902
Contact	SPG Demo NOC
Device Added	42 days 21 hours 11 minutes 16 seconds ago
Last Discovered	4 hours 49 minutes 45 seconds ago
Uptime	42 days 21 hours 48 minutes 48 seconds
Location	Main Datacenter
Lat / Lng	N/A

SNMP Fundamentals

Module 3: LAB

Labs

- Please follow the lab modules for
  - Lab 1: Net-SNMP
  - Lab 2: LibreNMS

Thank You!