

# SNMP

Introduction

Message Capture

Log Analysis

**SNMP**

Netflow

SNMP Traps

Proxy Services

Unified Threat Management

Authentication

Network Discovery

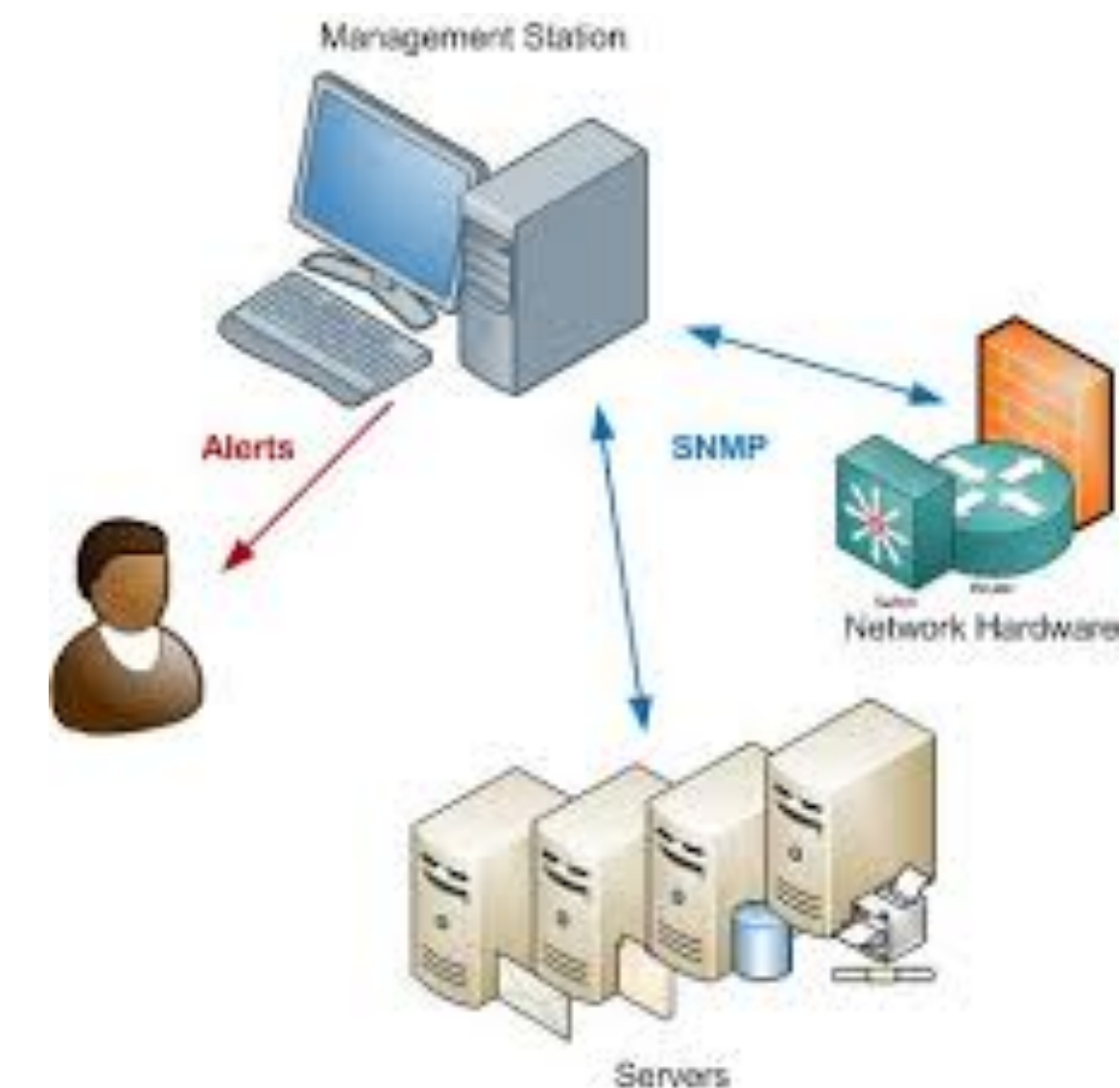
---

# Monitoring and Log Management

---

# SNMP Data Collection

- The Simple Network Management Protocol was created to provide a simple mechanism for remotely retrieving system information and changing settings
- It has been around a long time and the first versions did not take security into account, current versions do
- It is commonly set up with a single network monitoring station retrieving and storing data from agent programs running on hosts being monitored

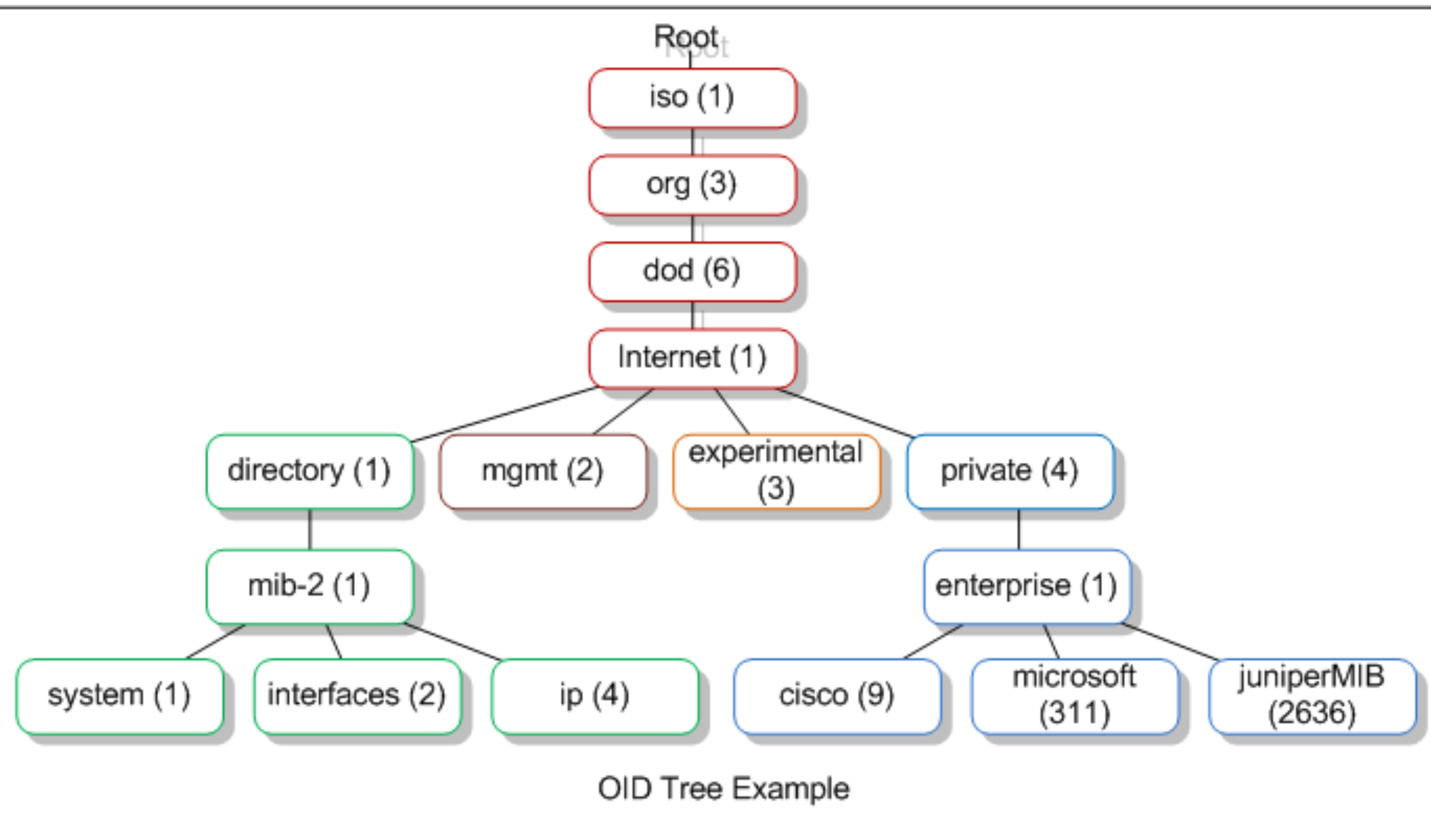


---

# Providing SNMP Data

- The `snmpd` daemon provides access to system information using SNMP as the protocol
- The Ubuntu agent can be installed with apt, package name `snmpd`
- The command line tools to access the SNMP service are in the `snmp` package
- The default config may restrict access to localhost and a limited dataset in read-only mode - it may also log every snmp request to syslog which is a lot of log entries
- The `dontLogTCPWrappers` directive can be set to `true` in the `snmpd.conf` file to only log failed snmp requests

# OIDs and MIBs



- An object identifier (OID) is the key used to specify a data element
- OIDs are hierarchical and specified using a numeric index scheme for each level of the hierarchy
- SNMP uses a management information base (MIB) to translate the oids from numeric index strings to names
- Install or update your mibs before using the snmp tools if you want translated oids
- [snmp-mibs-downloader](#) is the package on Ubuntu, download-mibs is the command to download them

---

# SNMP Access Control

- Community-based access, trivial names used to ask for access, no passwords in version 1 and version 2c
- User-based access controls with passwords and/or SSH/(D)TLS in V3
- Users and communities can be limited to views of the mib

---

# CLI Tools

- [snmpconf](#) - daemon configuration tool
- [snmpusm](#) - access control configuration tool (obtuse)
- [snmpstatus](#) - snmpd state reporter
- [snmpdf](#) - remote df using snmp
- [snmpnetstat](#) - remote netstat using snmp
- [snmpwalk](#) - mib browser
- [snmpget](#) - oid retriever

---

# snmpconf

- `snmpconf` is a configuration helper
- The `-g` option will run you through the basic config, asking you for settings to use
- `snmpconf` can be used to automatically add comments to your existing `snmpd.conf` file (`-a`)
- `snmpusm` can be used to add and remove users in your live configuration, but is difficult to figure out



---

# snmpstatus

- `snmpstatus` can be used to test whether a target host answers snmp connections
- If the host answers, some host identification will be displayed along with network statistics and warnings if any network interfaces are down
- Most snmp commands require a community and version to be specified on the command line using `-c` and `-v`
- Additional command line options for user authentication and encryption are required if you have v3 configured for auth or Priv modes



---

# snmpdf/snmpnetstat

- `snmpdf` allows you to get a summary of storage usage from a target host, including memory usage
- `snmpnetstat` allows you to run `netstat` on a target host via snmp
- `snmpnetstat` allows `netstat` command options using `-C`
- Requires community and version to be specified on the command line using `-c` and `-v`

---

# snmpwalk

- A MIB contains a great many potential data items in a number of formats
- Knowing which ones your device provides, and which ones have valid data in them can be challenging
- [snmpwalk](#) allows you to browse the data returned from an snmp agent and see the data items and values
- It is useful for identifying specific values to retrieve for monitoring purposes in scripts or management software packages
- Requires community and version to be specified on the command line using `-c` and `-v`

---

# snmpget

- `snmpget` allows you to retrieve a specific data item via snmp
- It can be used on the command line for quick tests
- It can be incorporated into scripts for automated monitoring
- Many monitoring packages use `snmpget` under the covers
- Requires community and version to be specified on the command line using `-c` and `-v`

---

# SNMP v3 Basics

- v3 adds authentication, encryption, and security models
- Security model can be user-based (usm), transport-based (tsm - tls, dtls, ssh), or kerberos-based (ksm) - usm is the most efficient and resilient to DoS but the most nuisance to maintain the configuration
- Users are created by stopping the daemon, modifying the [/etc/snmp/snmpd.conf](#) file to have [createUser](#) and [r\[ow\]user](#) lines, then starting the daemon, which makes [usmuser](#) entries in [/var/lib/snmp/snmpd.conf](#)
- Removing a user is done by stopping the daemon, removing the [createUser](#) lines from [/etc/snmp/snmpd.conf](#), the [usmuser](#) lines from [/var/lib/snmp/snmpd.conf](#), and optionally the [r\[ow\]user](#) lines in [/etc/snmp/snmpd.conf](#) for the removed users
- Alternately, you can use the [snmpusm](#) command to create the [usmuser](#) lines for your [/var/lib/snmp/snmpd.conf](#)



*Software can be chaotic, but we make it work*



*Expert*

Trying Stuff  
Until it Works

ORLY?

*The Practical Developer*  
*@ThePracticalDev*

# SNMP Lab

- Network Management Station setup
- Setup of snmp monitoring for all VMs
- SNMP V3 deployed