Monitoring Your Network with SNMP

For Wolverhampton Linux User Group

By Adam Sweet

What Is SNMP?

- Simple
- Network
- Management
- Protocol
- A platform independent way of presenting and retrieving system information and sending alerts over a network
- Primarily used for monitoring network connected equipment
  - Servers, switches, routers, printers, load-balancers, storage devices etc
- Simple does not necessarily mean trivial

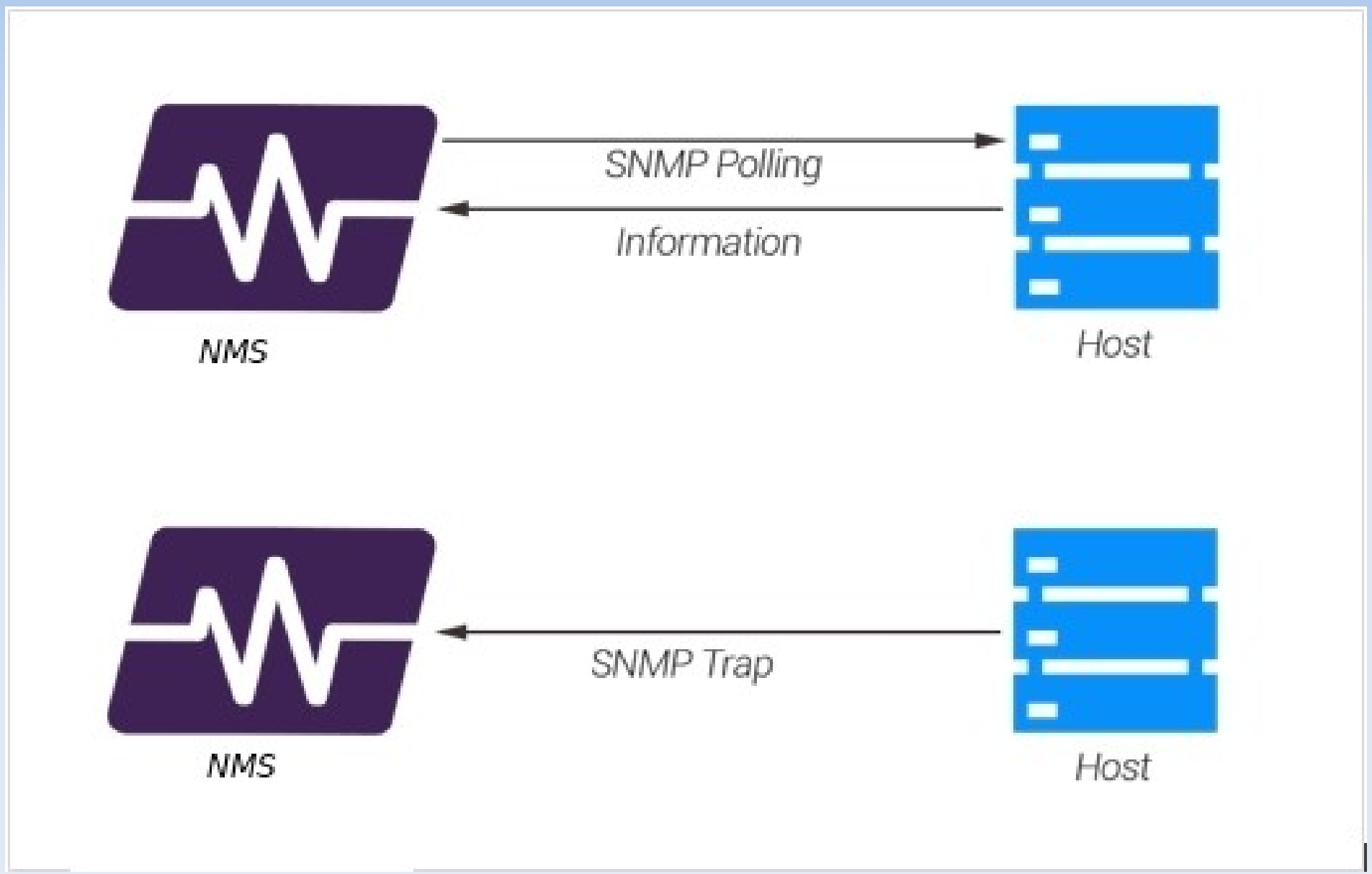
Retrieving Host Resource Info

- How do you find the CPU, memory, disk space, disk I/O, network card utilisation stats for a device?
- How can you monitor or graph it for all your systems in a single location?
- This information exists only inside the device itself
- They're not network services that we can connect to like HTTP or SMTP
- Many NMSes provide their own agents for Windows/Linux etc, but there aren’t NMS agents for everything
- If a system event occurs on a device, you may want it to send an alert out to the NMS rather than waiting for the NMS to notice
  - Perhaps it’s something so quick that an NMS would miss it
- SNMP is a standardised, platform-independent approach

SNMP Mechanisms

- There are two mechanisms to send and receive information using SNMP
- You can query a remote SNMP agent to retrieve information
- When you want a device to send an alert out when a system event occurs on it, this is called an SNMP trap
  - Traps are a bit involved for a short talk, perhaps we can cover them another time

SNMP Mechanisms



SNMP Agents

- The device you want to query must run an SNMP agent
- Any decent managed network device supports SNMP
  - Many terrible devices do too
- There is a Windows SNMP agent
- There is `net-snmp` under Linux and other agents for other Unixes
- Managed network devices have their own SNMP agents built in
- Your broadband router probably does
  - Your ISP may have hidden or disabled it

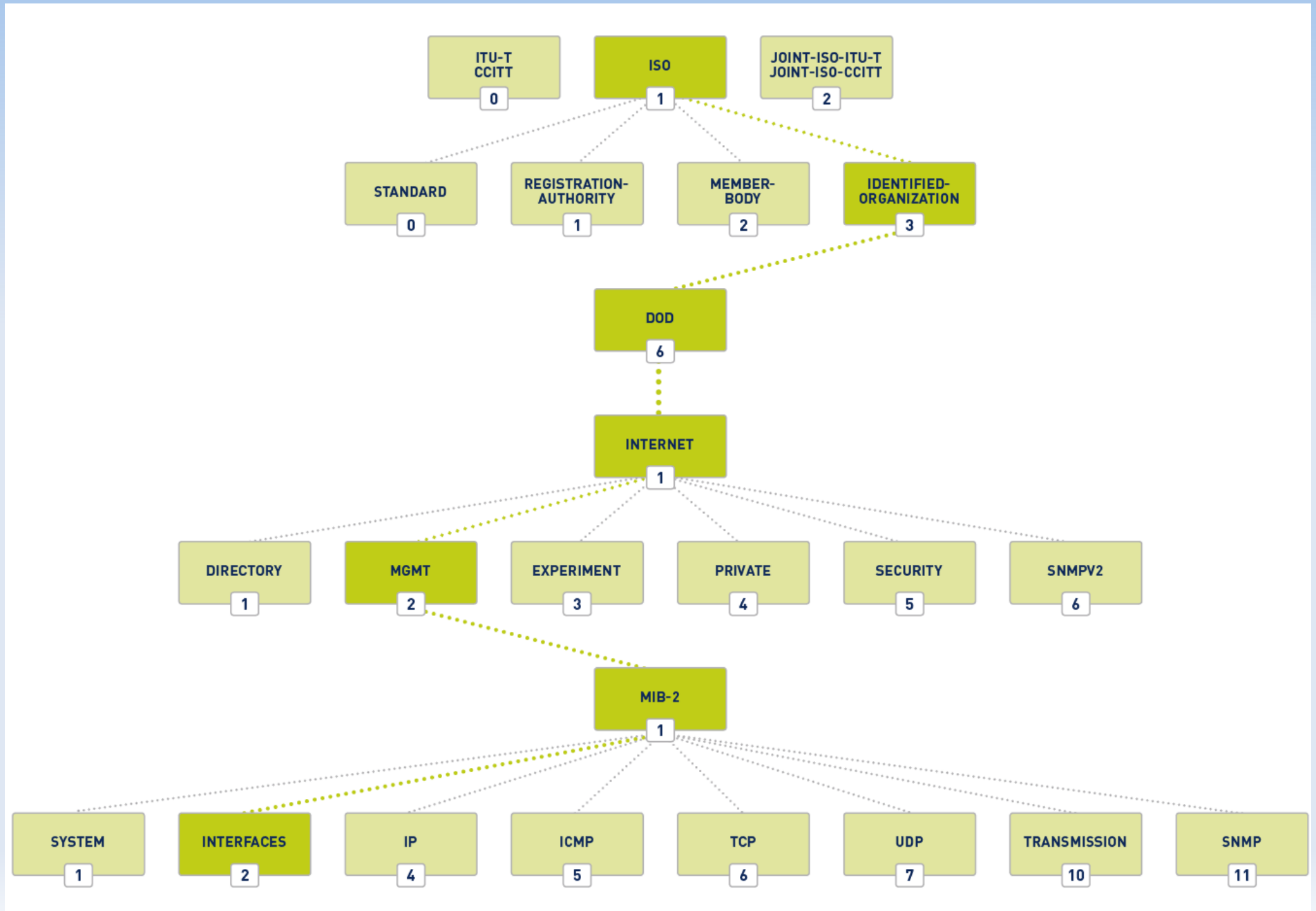
SNMP Management Software

- The system you will make SNMP queries from, or receive alerts on is called a Management Station
- In practical terms, that will be
  - A Network Monitoring System (e.g. Nagios, Icinga, Cacti, Solarwinds, HP Ops Manager, Prometheus, Bergamot etc)
  - A command line tool you run manually
- Most NMSes support SNMP monitoring
- Nagios has lots plugins that use SNMP to retrieve information

The SNMP Tree

- SNMP agents provide a tree of system resource information
  - (Disk, memory, CPU, network, running applications etc)
- It uses numeric hierarchy with (barely) human readable names for ease of use – like IPs and hostnames
- Each branch of the tree provides information on specific areas of system
- Each single item in the SNMP tree has an address called an OID (object identifier) which allows you to uniquely query it
- Each subsection of the tree is defined in what is called a MIB (management information base) which specifies the OIDs underneath it
  - MIBs are just plain text files that contain information in a specific format
  - There are thousands
  - A device will only support the MIBs it uses
- On each leaf node or end-point of the hierarchy is an OID with a value you can query

SNMP Hierarchy



SNMP MIBs

- SNMP MIBs define the contents of the SNMP tree and the OIDs used to call them
- An SNMP walk may not reveal everything on a device that is queryable over SNMP if you don't have the necessary MIBs or know the OIDs to query
- Many standard MIBs are already installed with the `net-snmp` package in `/usr/share/snmp/mibs/`
  - There is an Debian/Ubuntu package called `snmp-mibs-downloader` which will install lots of additional MIBs – useful for your management station or NMS
- You may need to download vendor specific MIBs and upload them to your management station or NMS for net-snmp to know about certain OIDs

SNMP Versions

- Version 1 was the original implementation
  - Only supports 32 bit counter values
  - A 1Gb interface can wrap a 32 bit counter in 34 seconds, so polling every 60 seconds is useless
  - No authentication or encryption – only use on private networks
  - Always use at least v2c, there's no benefit to using v1
- Version 2c
  - Essentially version 1 with 64 bit counters
  - You may need to explicitly enable it on some devices and you should
  - Again, no auth or encryption - only use on private networks
- Version 3
  - Adds authentication and encryption
  - More complicated to set up, we won't be covering it here

SNMP Primer

- SNMP runs listens on UDP/161 for queries and UDP/162 for receiving traps
  - They can be configured to use TCP though
- A running SNMP agent is configured with a community string (a plain text password)
- You need the following information to query it
  - SNMP version 1, 2c or 3 (2c or 3 preferred)
  - The SNMP community string
  - The device IP or hostname you want to query
  - The SNMP object you want to request (unless you walk the tree)
  - SNMPv3 requires a username, password, auth protocol, privacy passphrase and privacy protocol
- This info is a pre-requisite for any SNMP request

Installing net-snmp Tools

- To make snmp requests you need to install the net-snmp tools on your management station
- On Debian/Ubuntu and derivatives
  - `apt install snmp`
  - To allow numeric numeric ↔ human readable OID name translation you need to comment out the following line in `/etc/snmp/snmp.conf`:
    - `mibs :`
  - And install `snmp-mibs-downloader`
    - `apt install snmp-mibs-downloader`
- On Red Hat/CentOS/Fedora
  - `yum install net-snmp-utils`
  - Depending on OS version, you may need to use `dnf` rather than `yum`

Installing net-snmp Agent

- To make a Linux host queryable over SNMP you need to install the net-snmp agent
- On Debian/Ubuntu and derivatives
  - `apt install snmpd`
  - To allow numeric ↔ human readable OID name translation you must set the MIB path in `/etc/default/snmpd`:
    - `export MIBS=/usr/share/mibs`
    - `systemctl reload snmpd`
- On Red Hat/CentOS/Fedora
  - `yum install net-snmp`
  - `systemctl --now enable snmpd`

Configuring net-snmp Agent

- Before we can start querying, we need to configure the SNMP agent
- The default config is quite complex but it doesn't need to be
- Both Debian/Red Hat expect it to be in
  - `/etc/snmp/snmpd.conf`
- I use a far simpler net-snmp config
- Mine is already in place, after copying it there or changing the config be sure to start or reload snmpd
  - `systemctl reload snmpd`
- We can look at the config now

Querying SNMP Counters

- Resource usage counters are fairly standard in SNMP for CPU load, memory and network interfaces etc since the MIBs are standardised across many device types
- Cisco publish all of their MIBs, they are searchable and browseable
- The net-snmp commands for making snmp requests are `snmpget` and `snmpwalk`
- Syntax is:
- `snmpget -v <snmpversion> -c <community string> <target host> <OID>`
- `snmpget -v2c -c adamtest 192.168.10.250 1.3.6.1.2.1.2.2.1.2.2`
- `snmpget -v2c -c adamtest 192.168.10.250 IF-MIB::ifDescr.2`
- `snmpwalk -v2c -c adamtest 192.168.10.250`
- `snmpwalk -v2c -c adamtest 192.168.10.250 -On`
- The option `-On` option turns on numerical output, i.e.: no translation of the numeric ↔ human readable OID names takes place

SNMP Monitoring

- In your NMS, the easiest starting point is to use SNMP plugins which query what you want
  - The `nagios-plugins-snmp` package provides various SNMP plugins for Nagios, Icinga, Shinken and Bergamot etc
- Otherwise use the `check_snmp` plugin for specific OIDs
  - You'll need to know the OIDs you want to query
  - You can use `snmpwalk` with the `-On` option to get numeric OIDs
- The easiest way to find the OIDs you want is by Googling or speaking to your vendor and then snmpwalking
- You should know your NMS well enough to know how to tell it to check an SNMP metric
- You can prototype Nagios checks on the command line with `check_snmp` to get the options and thresholds correct before creating a command definition

Nagios SNMP Plugins

- There are plenty of SNMP Nagios plugins for different purposes in the third party plugin repositories
- https://exchange.nagios.org/
- https://exchange.icinga.com/
- My company also provide some
  - https://www.transitiv.co.uk/resources/monitoring-plugins
- Most SNMP plugins are written in Perl so you can see how they work

Graphing SNMP Stats

- Querying individuals stats manually isn't that helpful
- Having an NMS query them regularly is useful for alerting purposes
- Lots of the information available over SNMP lends itself quite nicely to being graphed
- There are many Open Source and proprietary tools that do so
  - Cacti
  - MRTG
  - Munin
  - Netdisco
  - The Dude
  - PRTG
  - Most commercial NMSes

Cacti

- As a quick demo, I'll set up Cacti
- In Debian/Ubuntu it's as easy as
  - `apt install cacti`
  - And answering the questions
- Log in at
  - http://yourserverip/cacti/
- Click Create > New Device
  - Provide the device name, IP and SNMP details
  - Click Save
- Click Create > New Graphs
  - Select the graphs you want to create
  - Select which counters to use
  - Click Create
- You can add more devices and graphs by repeating the process and selecting the device to add graphs for at the top of the New Graphs screen
- Now go view your graphs :-)

Further Reading

- Very good beginners reference to SNMP:
  - http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch22_:_Monitoring_Server_Performance
- O'Reilly Book:
  - Essential SNMP, 2nd Edition
  - by Douglas Mauro, Kevin Schmidt
  - Released September 2005
  - Publisher(s): O'Reilly Media, Inc.
  - ISBN: 9780596008406
  - https://www.oreilly.com/library/view/essential-snmp-2nd/0596008406/

Useful SNMP Links

- http://tools.cisco.com/Support/SNMP/do/BrowseOID.do
- http://www.oid-info.com/
- http://www.mibdepot.com/index.shtml
- http://www.oidview.com/mibs/detail.html
- https://www.manageengine.com/products/oputils/enable-snmp-cisco-router.html
- Your hardware vendor's documentation!