9 - Network Monitoring

As the network is the underlying infrastructure from which everything runs, and a system is only as fast as it's slowest component, the product being managed by the organization can only be as fast as the underlying network that serves it.

The pains of SNMP

What is SNMP? (Simple Network Management Protocol)

> Is a protocol proposed under RFC 1067 in 1988 for the purpose of monitoring and managing devices.

How does it work?

SNMP is a ADP-based protocol using ports 161 and 162. *Polling* occurs on port 161 (Inbound to the device), while *Traps* use port 162 (Outbound from the device).

There are two key concepts in a SNMP communication: The *agent* and the *manager*.

- *agent:* the device you want to get information from.
  - Process running in the OS of the network device you want to query (poll)
- *manager:* The device receiving that information.
  - Whatever is receiving the information from the agent

SNMP is often queried for data, but it also supports *traps*. (Similar to log events) A trap is emitted from the device what an event occurs and is sent to wherever you have configured traps th go.

There are multiple versions of SNMP in use, but the most common and widely adopted is "v2c". V3 is the latest version and implements encryption, but some smaller vendors still don't support it.

A word on security

SNMP is an insecure protocol, so the best way to secure SNMP is to architect security into your infrastructure, knowing that you are going to have a insecure protocol in use on it. The best way to do this is to build a management network into your architecture and allow SNMP queries to happen on the interfaces on that network only.

How do I use SNMP?

1. Install `snmp` package
2. Install the collection of MIBs `snmp-mibs-downloader`
3. Execute command `download-mibs` as root

4. Edit file `/etc/snmp/snmp.conf` and ensure `mibs +ALL` is in the file.

NET-SNMP package

Contains several command-line utilities. The most useful are:

- *snmpget:* retrieves a single OID
- *snmpwalk:* Enumerate a entire tree of OID's
- *snmpstatus:* Tests whether SNMP is functioning

Interface metrics

Network performance comes down to a few key factors: *bandwidth, throughput, latency, errors, and jitter*.

- *Bandwidth:* The theoretical maximum amount of information that can be pushed through a connection at once.
- *Throughtput:* The observed performance of a network link, also expressed in bits per second.
- *Latency:* The time it takes a packet to travel across a network link.
- *Errors:* Include metrics such as Rx/Tx errors, drops, CRC errors, overruns, carrier errors, resets, and collisions. Best monitor for physical issues with CRC errors and carrier errors.
- *Jitter:* The deviation of a metric from its usual measurement.

Interface and Logging

The syslog for a device also contains information about what interfaces are doing. The most interesting events are:

- Changes to trunk ports
- Ports becoming err-disabled
- Link aggregate interfaces becoming bundled or unbundled

Configuration tracking

Use tools such as RANCID to monitor your network device configuration files. When a configuration file changes, you can be notified by e-mail, slack, or any other method.

Voice and Video

Due to the underlying performance and inner-workings of the voice and video protocols, there is not much we can monitor and control. There is however three metrics we should be interested in monitoring. *Latency*, *Jitter* and *Packet Loss*.

The codec in use should be the same across the entire network.

Routing

Monitoring **static routes** is better achieved by monitoring the underlying links and the ability to pass traffic over the route (Using `iperf2`) than by monitoring for the existence of the route.

The most useful way to monitor **dymanic routes**, is by monitoring the dynamic routing protocols. (OSPF and BGP, primarily)

Spanning Tree Protocol (STP)

We want to keep track of when a change happened, so we suffice enabling logging at interface level.

There are two things we want to know:

- When a root bridge changes
  - Should happen rarely, if ever, so alert if it does change.
- When the protocol reconverges
  - More normal and acceptable, so the best way to monitor is to graph their occurrence.

Chassis

CPU and memory

Different devices will have different underlying behaviors, so graph them, but don't alert on them unless a vendor explicitly advises it.

Hardware

Monitoring switch stacks, line cards, supervisor cards, and power supplies is crucial.

One important thing to look for is cold start messages in your syslog. Cold starts represent a device having rebooted.

Flow Monitoring

Flow:

> A unidirectional sequence of packets that all share seven common values:
>
> 1. Ingress interface (SNMP ifIndex)
> 2. Source IP address
> 3. Destination IP address
> 4. IP protocol
> 5. Source port for UDP or TCP, 0 for other protocols

6. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
7. IP type of service

Flow monitoring is great for tracking down such things as high-bandwidth activities or nodes or analyzing bandwidth utilization on a per-IP, per-protocol, per-application, or per-service basis.

Capacity Planning

Capacity planning can be performed two primary ways:

Working backwards

This method is often used for when the business has hard requirements, and you need to determine how to implement. For example, if the business requires that a certain amount of data be transferred elsewhere within a certain amount of time, you can work backward to determine what size links are required to accomplish the goal. This method is not informed by any monitoring data.

Forecasting

Requires the use of data you've been storing in your monitoring system. This method is often used on a regular basis to upgrade links and hardware as the utilization grows over time. If you're making data-based decisions, your forecasting is straightforward: take at least the last six months of data and apply a trend line for the next however-many months. To apply the trend:

- Export data to excel, and use excel built-in graphing functionality
- If you are using *rrdtool*'s built-in trend forecasting
- If you are using *Graphite*'s built-in trend forecasting