# Meeting Abraham De Villiers

Position: Technical Specialist doing technical support; looks after the network

Years of Experience: More than 5 years

Estimate of 30 000 users on the wired connection (less users during vac)

# Investigation of Existing Tools in Use

Packages already exist: “What gaps are we trying to address?”

No tool is perfect (every tool has gap) and will offer everything you want end-to-end

## Tools:

* NTop - Freeware tool. Used to analyse traffic of Sflow; IP to IP; not platform dependant
* SolarWind for Flow
* CiscoPrime - Propietary software; used for configuration management
* Splunk - Takes text logs from various devices and contextualises the information; can show relationships between device
* Scom - Takes a long time to extract information; if there are network issues currently needed to be addressed, not the first tool of choice
* PingSweep - Runs a continuous traceroute; shows hop IP address and domain name; shows latencies currently experienced; shows packet loss (eg. if there are many deviations from the sample there is a problem at a certain hope)

Tenet making use of most of the tools mentioned.

## Questions:

* “What is the difference between Sflow and Netflow?”
  + Depends on speed of link.
  + Sflow can be made use of for higher speeds - sample of traffic is used and need to extrapolate results.
  + Netflow handles real-time collection but (can) fall short if traffic is too high volumes.

# Description of Network Problems

“Need to get access to information where the problem occurs as soon as possible to avoid speculation. Often a case of a problem changing or appearing to be solved before it is addressed”

* What metrics are used for the network performance depends on the context of the problem
* To find hops: Log onto router to see routing table

# Visualisation

## Existing Tools and Vis

* Topology Visualisation shows all devices and how they are connected to each other
* Can determine how much is web browsing
* To show flows:
  + Thickness of lines
  + Colour
* Busy nodes can easily be identified with colour and thickness of line.
* Geolocation data available where each country flag is shown in a circle on screen connected by lines
* Tools are interactive
  + Can explore data
  + Drill down available
  + Level of detail depends on what you are trying to achieve

## Proposed Idea

Dashboard is useful to see all info at the same time on one screen as opposed to many monitors (only big corporations able to do this)

# Misc Info

* NRENs have an international pipe and want to know where traffic goes and what applications using that traffic.
* UCT’s traffic capped by Tenet