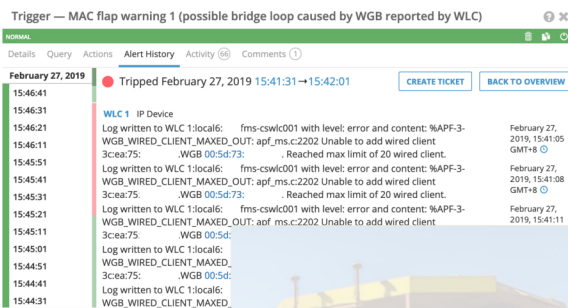


Case Study

Using IMS to catch and alert on the presence of a switch loop, before it occurs!

The Operation

The subject of this case study is a mine in the Pilbara region of Western Australia. It consists of over 45 Autonomous Haulage Trucks (AHT's) and over 1000 connected devices to keep the system running. This large open-pit iron ore mine is reliant on it's network stability for smooth 24x7 operations.



The Problem

A Switching loop or bridge loop occurs in computer networks when there is more than one Layer 2 (OSI model) path between two endpoints (e.g. multiple connections between two network switches or two ports on the same switch connected to each other). Configuring a Cisco wireless client generally requires a technician to connect to the radio via a console cable and laptop. Connecting the radio to the network is the next step. The way the radios were being commissioned, was by plugging the radio in to the network using an Ethernet cable. If the technician isn't careful it can create a switch loop. In this case it is via the Ethernet cable plugged into the radio and over the air via the WiFi link. The resulting impact to operations can be an outage of multiple hours, sometimes days. The resource scramble to fix the issue is something IMS addresses.

The Solution

The development team as well as network engineers from FTP Solutions, were able to identify indicators in the syslog's reported by the Wireless LAN Controller (WLC) and produce a trigger/alert based on this. By being able to actively alert on not only the issue that is occurring, but also being able to identify which device is the root cause, meant that the operation could reduce its MTTR enormously for events of this type. By using IMS in this way, as a predictive alerting platform, the company became inspired to go on and implement this ethos with other technology related issues that had been plaguing their operation for years.