Managing Cisco IOS devices

You are a network engineer working closely with network operations center (NOC) analysts. You are looking for ways to monitor the state of your Cisco switches and routers and know that Splunk software has effective correlation capabilities. The Cisco network manager software is useful with specifics of the products it's designed to manage, but the NOC and IT would like a way to correlate alarm conditions in the network with impacts to other business services that depend on the network. You can use Splunk software to identify and resolve potential problems in your Cisco devices, such as duplicate IP addresses, duplex mismatches, overheating, and port flapping. You can also monitor log volume and other performance indicators.

Data required
Cisco IOS

How to use Splunk software for this use case

You can run many searches with Splunk software to manage Cisco devices. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Duplicate IP addresses in Cisco IOS devices
- Duplex mismatch in Cisco IOS devices
- High temperature alarm in Cisco IOS devices
- Cisco IOS devices with highest log volume
- Port flapping on Cisco IOS devices

Next steps

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Log collection with syslog
- Integration of Splunk dashboards and reports into the Network Operations Center (NOC)

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Reduction of mean time to problem resolution
- Reduction in network related ticks submitted by end users

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf talk: IT services modernization at Cisco: How Cisco monitors three million devices daily with Splunk
- App: Cisco Networks App for Splunk Enterprise