Port flapping on Cisco IOS devices

Port flapping is a situation in which a physical interface on the switch continually goes up and down, three or more times a second for at least 10 seconds.

Common causes for port flapping are bad, unsupported, or non-standard cable or other link synchronization issues. The cause for port flapping can be intermittent or permanent. You need a search to identify when it happens on your network so you can investigate and resolve the problem.

Data required

Cisco IOS

The Cisco IOS system message logging process uses the syslog protocol to send important messages to remote logging services, such as Splunk. The required add-on expects the data stream to be assigned the syslog sourcetype by the input configuration and will rename it to cisco:ios in the transformation configuration. For details on how the transformation is implemented, see the props.conf and transforms.conf in the add-on and the Splunk documentation. For more information on syslog and Splunk, see the (SYSLOG) Syslog Data Collection section of the Splunk Validated Architectures white paper.

Procedure

Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
| eventtype=cisco_ios-port_down OR eventtype=cisco_ios-port_up product=IOS
| eval port_state=if(vendor_action="up",1,0)
| stats sparkline(sum(port_state),15m) AS trend count, latest(vendor_action) AS current_port_status BY host,src_interface
| eventstats sum(count) AS host_total BY host
| sort -host_total -count
| fields -host_total
| table host,src_interface,trend,current_port_status,count
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

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.
**Splunk Search**

```
| eval port_state=if(vendor_action="up",1,0)
| stats sparkline(sum(port_state),15m) AS trend count,
      latest(vendor_action) AS current_port_status BY
      host,src_interface
| eventstats sum(count) AS host_total BY host
| sort -host_total -count
| fields - host_total
| table host,src_interface,trend,current_port_status,count
```

**Explanation**

- Search for port up and port down events in all Cisco IOS data. Eventtypes are supplied by the TA
- Further constrain results to where product is IOS
- Evaluate the port state as 1 if the status is "up", and 0 otherwise. These numeric values are needed later to calculate the trend with the sparline.
- Create a trendline of port statistics over the last 15 minutes.
- Calculate a running total number of port flaps for each host.
- Sort the results by host total and secondarily by message count, with the highest values first.
- Remove the host total field from the results.
- Display the results in a table with columns in the order shown.

**Next steps**

The following sample result from the search shows the host, source interface, current port status, and the count for the host. The sparkline is not shown below but would be rendered by Splunk.

<table>
<thead>
<tr>
<th>host</th>
<th>src_interface</th>
<th>current_port_status</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>cph-c-001-rtr-1</td>
<td>Ethernet1/0/46</td>
<td>up</td>
<td>7</td>
</tr>
<tr>
<td>host</td>
<td>src_interface</td>
<td>current_port_status</td>
<td>count</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>---------------------</td>
<td>-------</td>
</tr>
<tr>
<td>hel-c-001-rtr-1</td>
<td>Ethernet1/0/46</td>
<td>up</td>
<td>5</td>
</tr>
<tr>
<td>osl-e-310-swi-1</td>
<td>Ethernet1/0/46</td>
<td>up</td>
<td>5</td>
</tr>
</tbody>
</table>

Finally, you might also want to look at similar searches in our article [Managing Cisco IOS devices](#).