September 10, 2019

SYSTEM AND METHOD OF LINK PROTECTION FOR FIBER OPTICS

Amitesh Shukla

Manish Jhanji

Vinod Cherukatt

SYSTEM AND METHOD OF LINK PROTECTION FOR FIBER OPTICS

AUTHORS:
Amitesh Shukla
Manish Jhanji
Vinod Cherukatt

ABSTRACT

Techniques are described herein for a network manager driven approach to identify and predict link level issues using Digital Optical Monitoring (DOM), Digital Diagnostic Monitoring (DDM), and/or fiber cable data available on a per port basis. Techniques described herein include a mechanism that can identify small form-factor pluggable (SFP), enhanced SFP (SFP+), quad SFP (QSFP), etc. issues in advance and take proactive appropriate actions to fix and/or mitigate link level issues; thereby resulting in improved transceiver (xcvr) assurance.

DETAILED DESCRIPTION

In general, the DOM/DDM feature enables monitoring key operating parameters on an interface, such as transceiver temperature, supply voltage, transmit (TX) bias current, TX output power, and received (RX) optical power. As per the SFF-8472 Specification, there are bits reserved for future use so there is a possibility that additional parameters may be available for diagnostic and monitoring. Typically, device monitoring and diagnostics can be enabled either globally or on per port basis.

Research has identified that these operating parameters can directly and/or indirectly influence the operation of connected optics and deviation from predefined threshold(s) can result in issues like link flap, link down, traffic errors like Frame Check Sequence (FCS) errors, laser degradation, etc. Apart from the link level impacts, the temperature of the transceiver impacts the overall temperature in the cage. Further, bugs such as persistent FCS errors on an Ethernet interface can occur in cases of significant optical attenuation.

Currently, alarms and warnings are handled by informing a customer, user, etc. via a syslog, etc. when certain operating parameters go below, or above certain vendor defined

threshold(s). However, such mechanisms are mostly reactive and typically do not trigger any action to mitigate a problem.

Companies are investing and moving towards intelligent networks in which issues occurring on networking devices can be predicted in advance and fixed, if possible. To achieve this, there is a need to identify various network level problems and provide solution(s) to rectify them, which collectively can be treated as a healing network. Thus, there is a growing demand to provide network assurance by utilizing meaningful and actionable insights from the data generated on networking devices.

Since internal and/or external factors, when combined (e.g., creating a complex combination of various factors), can directly and/or indirectly influence the operation of optics and, hence, a network link. Such link level issues can result in merchandise returns without much explanation and insight. Sometimes, it can be very difficult to simulate similar environments in a customer/user network or in a local lab to reproduce such link level issues.

This proposal provides a network management system driven approach/mechanism to identify and predict link level issues using DOM/DDM data available on per port basis. This approach/mechanism can potentially identify issues related to SFP/SFP+, etc. in advance and take appropriate actions to fix/mitigate them.

In particular, this proposal provides a mechanism to facilitate the identification and prediction of link level issues using DOM/DDM and connected fiber data. Figure 1, below, is a sample of DOM/fiber cable data available that may be available for an optical device. It is to be understood that the data shown in Figure 1 is only one example of data that may be available on a device; different devices may have different capabilities and may have different/additional data that can be collected.

```
N7K-1# sh int ethernet 1/10 transceiver details
Ethernet1/10
    transceiver is present
    type is 10Gbase-SR
    name is CISCO-AVAGO
    part number is SFBR-709SMZ-CS1
    revision is G4.1
    serial number is AVA1732A0JK
    nominal bitrate is 10300 MBit/sec
    Link length supported for 50/125um OM2 fiber is 82 m
    Link length supported for 62.5/125um fiber is 26 m
    Link length supported for 50/125um OM3 fiber is 300 m
    cisco id is --
    cisco extended id number is 4
    cisco part number is 10-2415-03
    cisco product id is SFP-10G-SR
    cisco vendor id is V03
    number of lanes 1

           SFP Detail Diagnostics Information (internal calibration)
  ----------------------------------------------------------------------------
               Current              Alarms                  Warnings
               Measurement     High        Low         High          Low
  ----------------------------------------------------------------------------
  Temperature   18.03 C        75.00 C     -5.00 C     70.00 C        0.00 C
  Voltage        3.31 V         3.63 V      2.97 V      3.46 V        3.13 V
  Current        5.32 mA       10.50 mA     2.50 mA    10.50 mA       2.50 mA
  Tx Power      17.80 dBm      21.69 dBm    8.69 dBm   18.69 dBm     12.69 dBm
  Rx Power      17.06 dBm      22.00 dBm    6.09 dBm   18.99 dBm     10.09 dBm
  Transmit Fault Count = 0
```

Figure 1

As discussed above, various research points to a direct impact of transceiver parameters such as temperature, voltage, etc. on link stability. Mining this data can help to predict an anomaly and/or degradation in the link.

Link level degradation predictions made in advance using DOM data analysis can help take appropriate action such as, for example:

- Adjusting the cooling on a device to keep the temperature of the optical module within accepted range, when predicted to go beyond a threshold.
- Bumping up the transceiver log level for predefined duration(s) to capture additional information if the system predicts a link level behavior change.

- Invoking software recovery mechanism(s) such as redirecting any critical traffic on a given port to another port, etc. in case link flap/down is predicted based on the data analysis.
- Providing recommendation(s) with detailed insight to an administrator rather than just providing a syslog alarm, as is typically provided in systems.
- Using pattern(s), which may help to identify any rogue/defective optical module (often breaching a threshold) on a device if a certain anomaly is identified on a particular port based on the analysis. In such cases, action(s) could include shutting down a port apart from notifying an administrator.

Although, taking actions on the basis of vendor defined threshold may work well in some cases, vendor defined thresholds themselves may not provide accurate range when many different parameters are under consideration. For example, a temperature threshold up to which a certain module can work well may be much lower than the vendor threshold when other parameters start deviating at the same time.

Thus, a mechanism is needed that can capture different variations and combined effects on a link based on data generated from a diverse set of devices, from different optical modules/fiber cables deployed in extremely diverse environments (e.g., from regular office space to industrial setups operating in harsh environments).

This proposal includes a Machine Learning (ML)/Statistical based method to:

- Identify threshold ranges (when multiple factors are in play), on a per port basis. Regression models such as linear regression can be deployed for threshold predictions;
- Classify and predict link status as GOOD, FLAP, or DOWN. This can operate as a classification model that uses the data to classify whether a link is going to remain operational or will be impacted. This can be a periodic process checking the link status at regular intervals or can be triggered based on predefined events; and
- Deploy time series classification and forecasting models to capture data variances. For example, there are other external factors that can impact link operation. Many of these factors are temporal in nature and changes with time.

For example, traffic load may be different at different times of the day, or the temperature under which a device operates may have some fluctuations as seasons change, etc. To handle such variations this, proposal provides for deploying time series classification and forecasting models to capture such data variances.

Various data types that may be captured/analyzed according to this proposal can include, but not be limited to, DOM data such as temperature, supply voltage, TX bias current, TX output current, received optical power, various threshold levels, etc. and external data, such as inlet temperature, outlet temperature, onboard sensor data, external sensor data, etc.

For this proposal, operations provided via a network management system can include treating link level problems as imbalanced data problem where true positives may be rare. Imbalanced data set handling mechanisms in the ML pipeline on the network management system can handle producing appropriate input data which can be fed into a model training step. Further, different policies such as oversampling, under sampling, threshold moving, etc. can be adopted by the network management system for handling imbalanced data.

Once the data is prepared, a transceiver (xcvr) assurance engine trains the model and/or predicts the link state, thresholds, etc. In at least one implementation, on link failure/anomaly/flap prediction, the network management system can prepare a message with failure signature, device information, port information, SFP type, etc. and can send the message to the impacted device for further action(s).

For this proposal, a configuration can be provided for devices in a network to enable/disable features described herein (e.g., for collecting data, etc.), which can include providing a per port basis of control where the features can include tagging participating and non-participating ports that may provide data for the analytics.

Figure 2, shown below, illustrates various operations and/or features that may be performed and/or provided via a network management system in order to facilitate techniques provided by this proposal.

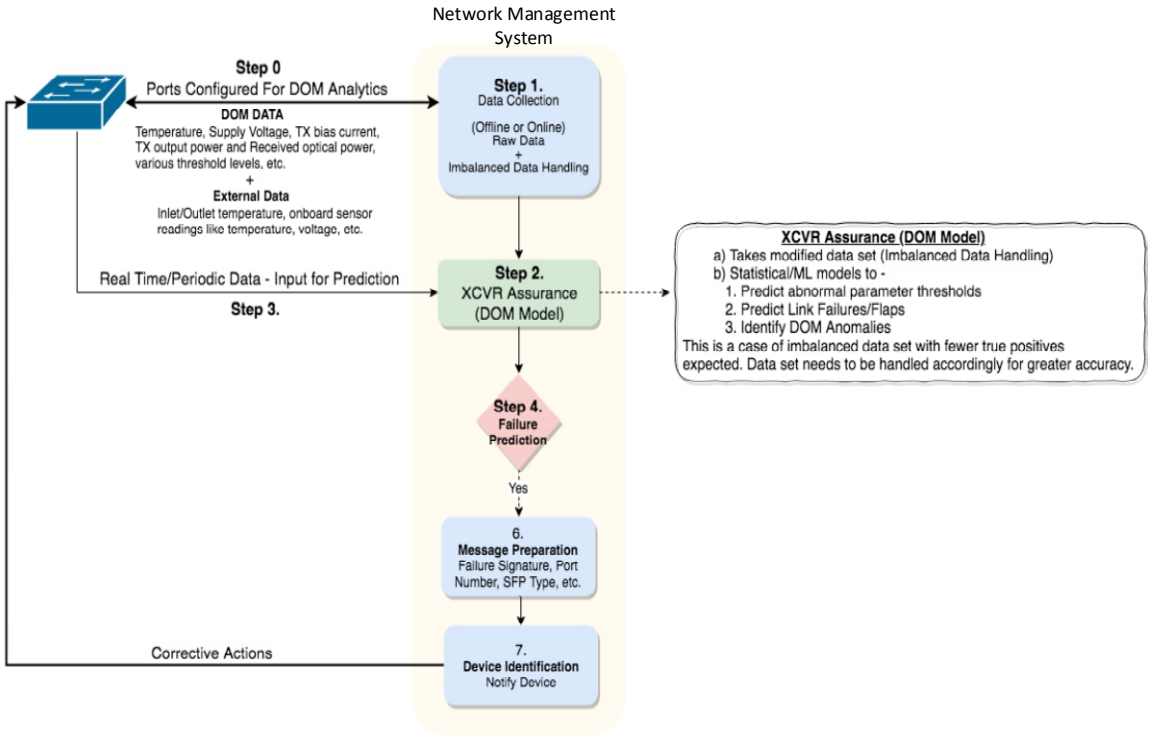

Figure 2

In summary, techniques are described herein for a network manager driven approach to identify and predict link level issues using DOM/DDM/fiber cable data available on a per port basis. Techniques described herein include a mechanism that can identify SFP/SFP+/QSFP/etc. issues in advance and take proactive appropriate actions to fix/mitigate link level issues; thereby resulting in improved transceiver assurance.