How to Troubleshoot Your Network Starting from the Physical Layer

While starting your network troubleshooting from the software layers might seem like a good enough idea on the surface, (unless you're keenly aware of deliberate changes that have been made) it can be the difference between being shrouded in a haze of panic and frustration vs. diligently identifying and rectifying whatever's disrupting your network.

Taking a logical and proven approach that focuses on the physical layer first can save you tremendous amounts of time and energy when it comes to getting your network back in order.

Take a quick look at the Open Systems Interconnection (OSI) model to visualize the separation of network communications and the order that they build upon each other. From highest-to-lowest, those layers are as follows:

- Application Layer (Software Layer)
- Presentation Layer (Software Layer)
- Session Layer (Software Layer)
- Transport Layer
- Network Layer (Hardware Layer)
- Data Link Layer (Hardware Layer)
- Physical Layer (Hardware Layer)

We're going to begin troubleshooting at the P\physical layer because this layer is most subject to outside influences.

What to do When There are Errors:

When a link drops or takes errors, the impacted transceivers and platforms are your first clues in discovering what's gone wrong.

First, review your logs to see what was going on at the time of the incident. Most transceivers have Digital Diagnostics Monitoring (DDM) for inspecting elements of the relevant device.

Your DDM shows what power the transmit has, what value the receiver is seeing and other potentially helpful insights such as temperature and power statistics.

These values are not always considered a perfect reference; however, they can provide a basic diagnostic of what's going on.

If the transceiver indicates a warning or an alarm, you're that much closer to discovering the issue at hand.

Verifying the Diagnostics

Now, using your preferred light meters, it’s time to verify whether what the transceiver told you is true or not.

- Is there or isn’t their light coming through?
- Is the transceiver producing the signal it believes?
- Do the Tx and Rx values align with the internal accounting?

Various light meters are used for different types of transceivers. The most widely adopted CWDM, DWDM and Graywave transceivers benefit from using the correct meter to accurately measure their Tx and Rx signals.

If your transceiver and meter both agree on the diagnostics, then it’s safe to assume their telling the truth of the situation.

When Your Transceiver and Meter Disagree

When the transceiver and meter disagree, there is generally a common culprit -- surface contamination.

It’s stunning to realize how little it requires for an endface to become contaminated. Tiny specks just outside of the operational area can spread because of ambient vibration and disrupt your networks at the worst possible time.

This is why it’s essential to properly **clean** all mating surfaces any time connections are examined or made.

Use a fiber scope to rid yourself of any contamination doubt with direct inspection of your fibers and optics.

Fiber scopes like the **Integra SmartProbe Wireless 2** provide automatic qualification that the endface is cleaned appropriately.

Validating the Fiber

The next step requires validating the fiber itself. Before you check the full transit, start by validating your fiber locally using a tool like the **Visual Fault Locator** (VFL)

The VFL shines a bright visible light down the fiber allowing you to identify any breaks or bend damaged areas via a glow, even through the fiber’s jacket.

If/when you identify a damaged area, ensure you use reliable replacement fibers to repair the damaged area. Running a temporary jumper that isn’t the correct length, although it may appear quicker in the moment, only transforms a single outage into multiple outages either immediately or in the not-so-distant future.

Up Next, the Optical Time Domain

Once you’ve verified everything is in working order on-site, but you know there’s still a signal issue, then it’s time to press onward with the **Optical Time Domain Reflectometer** (OTDR).

The modern OTDRs shoot a laser down a fiber, and then record the reflections and their characteristics.

The two things to be aware of when using an OTDR are as follows:

- One, The OTDR must “shoot” on a fiber that does not have a signal on it. Meaning, you must either remotely shut down or manually disconnect the far side.

- Two, the beginning of a fiber shot has a blind area that sacrifices accuracy, so you must use a launch reel to get accurate data for the fiber you’re testing.

Now that you’ve accounted for the two items above, you can reliably gather the easy-to-read information presented by the OTDR to better understand the issue(s) facing your network.

In a real emergency outage situation, you more than likely won’t be able to compare history OTDR reports against the readings you’re faced with, but network issues are often not so subtle when dealing with fiber damage on a path.

Conclusion

It can be overwhelming to confront abstract network problems, however, taking the effective approach of troubleshooting your network from the physical layer first (with the right tools and the right approach) can ensure you and your network pragmatically overcome chaotic events every time.

If you’re interested in additional support or want to discuss ways to better troubleshoot your network with the right tools and approach, **reach out to your Integra sales or engineering team**.

May your network be trouble-free and your on-call periods be quiet!