Comprehensive Sourcing Solutions for Optical Transceiver Modules

Introduction

Cisco's optical transceiver modules are qualified in accordance with the most rigorous requirements in the industry. Before their release, the suppliers and their products must pass rigorous qualification tests and requirements which can't be matched outside of Cisco.

This paper is intended to help you understand Cisco's thorough approach to optics sourcing and qualification. You benefit from this whether you use Cisco or non-Cisco host switches and routers.

Contents

Background

Standards

Optical Interface

Form Factor

Testing

System Level Qualifications

EMI/EMC Compliance

Reliability and Manufacturing

Benefits

Security of supply

Service

Case Studies

Myths

Conclusion

Learn more

Background

Cisco was instrumental in starting the now common practice of using pluggable optics in switches and routers. The reasons were clear. At the time (late 1990's), Ethernet bandwidth had risen to 1Gb/s and fiber optics could carry signals farther than copper cables. Pluggable optics enabled end users to use modules optimized for different speeds and reaches and allowed for easy repair if the transmitter laser failed. They also provided the option to add capacity over time, as needed.

IEEE standardization of the Gigabit Ethernet physical layer and MSA specification of form factors, such as SFP, enabled multiple manufacturers to enter the pluggable optics market. While standardization carries many benefits, it is a common misconception that all products on the market are identical. Many problems that transceiver modules create in Cisco host platforms can only be discovered at Cisco test labs. These are routinely detected during qualification and corrected before product release. Additionally, we have witnessed numerous accounts of field issues that are traced to non-Cisco transceiver modules. These issues would likely manifest over time if they aren't uncovered during our qualification process, regardless of whether the transceiver modules are used in Cisco equipment or not.

Quality of service is a key business driver, especially for top tier service providers. We go beyond common industry practices to ensure transceiver modules meet all the quality, reliability, and functional requirements when plugged into a Cisco host platform. Technical services are an integral part of the solution. These services offer unparalleled support in the form of live troubleshooting and same day replacement through our well-known Technical Assistance Centers (TAC).

In this paper we explore Cisco's approach to protecting customers from issues related to pluggable optics. Our comprehensive process has been developed over the course of two decades and leverages technical expertise, high volume, and supply chain experience. It ensures that high quality optics are available when you need them.

Standards

Pluggable transceiver modules for Ethernet must follow industry standard specifications for protocol and form factor. The two are described here.

Optical Interface (Physical Medium Dependency)

Most physical network interface requirements, also known as PMDs, are defined by the IEEE 802.3 working group. Various standards are categorized by reach and speed; for example, 10GBASE-SR, 25GBASE-LR, 100GBASE-SR4, and 100GBASE-LR4. Standardization is intended to enable interoperability between devices from multiple vendors (Cisco, Juniper, Alcatel-Lucent etc). Not all interfaces are standardized by IEEE, however.

Multi Source Agreements (MSA) at 100G, such as CWDM4 and PSM4, have been popular in data center applications.

Form Factor

A form factor MSA is defined by a group of transceiver manufacturers so that participants can adhere to a common module form factor specification (SFP+, SFP28, QSFP+, QSFP28, etc). Form factor MSA specifications typically include mechanical requirements with tolerances for the host port as well as the transceiver. Electrical requirements for low speed module management signals are also included, leaving high speed signal specifications to the optical interface standard. While form factor MSAs do enable interoperability between host ports and pluggable modules, they do not guarantee that transceivers from all manufacturers have the same performance.

Testing

Specifications of Cisco transceivers encompass all of the requirements in the optical interface and form factor standards, plus additional requirements needed for the transceiver to operate reliably on Cisco and non-Cisco platforms. These transceivers go through the Cisco Qualification Process outlined in Figure 1.

The qualification process is rigorous and prototype samples routinely fail. Failure at any step forces a thorough review, resulting in design modifications for additional margin or elimination of manufacturing inefficiencies.

The QSFP28 and SFP28 form factors have presented additional failure modes, partly due to their higher data rate per lane (25G), but also because of the adoption of additional technology such as Forward Error Correction (FEC) and Continuous Time Linear Equalization (CTLE). As we look forward to the introduction of 400G form factors, such as QSFP-DD, complexity only increases, making it more critical to thoroughly test and qualify.

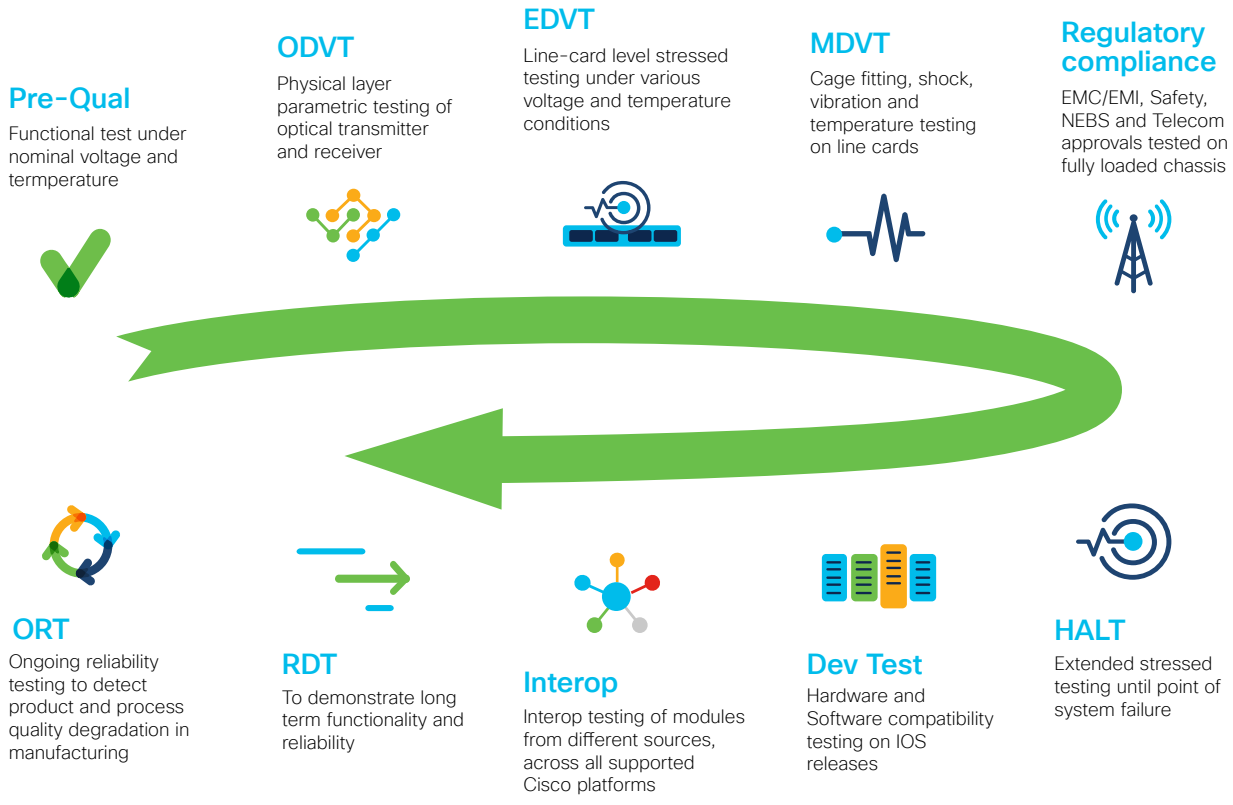

Figure 1. Cisco qualification and reliability testing process.

System level qualifications

It is a common misperception that because the optical interface specifications and form factors are standardized, there is absolute uniformity among various manufacturers' transceiver modules. In reality, there is wide variation among the products on the market, and many of the problems are specific to a system platform design.

Cisco performs extensive system-level qualification and compliance testing of optical transceivers on fully-loaded Cisco platforms. This includes module/host integration qualification over the entire range of operating conditions for optical, electrical, and mechanical performance.

Decades of stress tests with our diverse platform portfolio has allowed us to accumulate a knowledge base that increases module design margin and fosters robust design practices. This helps accommodate the inevitable variations in platform designs. Therefore, the risk of incompability is significantly reduced even on untested platforms such as non-Cisco hosts.

The system-dependent problems that can arise are numerous. They include, but are not limited to the items in Table 1. All of the issues in Table 1 have been observed during qualification testing and in the field on third party optics. If they are caught during qualification, they are corrected in a subsequent design iteration before the release of the product.

Table 1. Common errors found during qualification testing. Many problems are only detectable during system-level tests, even though the modules are technically MSA compliant.

Problem	Description	System-dependent?	Impact to user
Link-flap	Interface goes up and down intermittently.	Yes	Not acceptable for normal network operation. Intermittent problems can be difficult to debug.
CRC errors	Indicates data transmission errors.	Yes	Link not usable.
Inrush current issues	Power supply voltage not stable during power up.	Yes	Can cause link to go down, or never come up.
Overheating	Module is not cooled sufficiently.	Yes	Degrades module lifetime and reliability.
Mechanical issues	Module does not fit in host port, even if MSA compliant.	Yes	Module gets stuck in the port, or doesn't engage when plugged
Hot-plug issues	Link may not come up when hot-plugged	Yes	Module may not be usable.
EMI/EMC noncompliance	Stray radiation due to insufficient mechanical shielding	Yes	Can cause wide range of problems, like data errors and link-flap
EEPROM errors	Factory writes incorrect settings to EEPROM memory registers. Some registers are Cisco-specific.	Yes	Can prevent module from being recognized by host platform
Reliability test failure	Module fails during accelerated aging test.	No	Module will fail prematurely in field.
I2C	Timing errors, byte read errors.	Yes	Module may not be usable.
Platform software compatibility issue	Host may not communicate with module, or not recognize.	Yes	Module may not come up, or may not be usable.
DOM accuracy	DOM (Digital Optical Monitoring) parameters not meeting spec.	No	Real-time monitoring not reliable.
Power consumption	Module consumes too much power.	Yes	Module may overheat or cause system power issues.
Interoperability	Traffic errors when specific combinations of vendor modules are paired.	No	Despite meeting standards specifications, transceiver vendor design variations can still result in incompatibilities.
CDR	Link flaps due to unretimed signals	Yes	CDR design parameters or default settings in the module may not be compatible with host software or hardware design.

For example, Cisco software detects the transceiver module type based on the transceiver code, defined by the form factor MSA, that resides in the module's EEPROM programming. For some optical interfaces, the transceiver codes are not defined; we use a proprietary table of extended ID's to recognize the module type in these instances.

For newer form factors such as QSFP28 and SFP28, equalization is needed on the electrical interface lines between the module and the host. This is known as Continuous Time Linear Equalization (CTLE) and when equalization parameters are not aligned, traffic does not pass error free. Clock data recovery (CDR) circuits tend to be more complex and the initialization sequence that the host uses to bring up the module becomes more complicated. Also, at the higher data rate, different ports on the same host may or may not contain additional circuitry depending on the trace length between the ASIC and the port. Therefore, successful testing on one port of a host platform may not necessarily qualify a different port in the same host platform.

EMI/EMC Compliance

An MSA compliant transceiver module may still violate electromagnetic interference and electromagnetic compatibility (EMI/EMC) regulations when plugged into a host port. EMI/EMC radiation is regulated by the FCC so that any unintentional radiation does not interfere with other equipment and legitimate transmissions in wireless and radio bands. Cisco transceivers are tested in fully populated worst-case linecard configurations inside Cisco hosts. The mechanical design of the Cisco transceiver and the port are both optimized by means of several design iterations & system-level testing. Since the transceiver plugs into a port (hole) on a switch router, the mechanical fit is critical to meet the radiation and emissions compliance, as required by law. We maintain country specific compliance testing results for Cisco platforms with the optics.

As data center switches grow in port density, more transceivers are active and generate more risk of radiation. Therefore, the limits on each individual transceiver are tighter. They must be well shielded and not allow air gaps between the module walls and the host port cage. Furthermore, as data rates increase, the higher frequency bands involved are more difficult to test.

Compliance is important for more than satisfying legal regulations. Systems failing to meet these radiation and emission standards could cause failures in nearby equipment. Stray radiation is often the root cause of intermittent failures on the switch/router itself, such as link-flap and CRC errors. By ensuring compliance, the risk of functional problems is greatly reduced.

Reliability & Manufacturing

We have a comprehensive reliability testing policy, both prior to product release and ongoing reliability testing of the manufacturing line. This ensures that the performance and reliability specifications are met under all stated operating conditions and over the lifetime of the Cisco transceiver product.

Benefits of Cisco Optics

Security of supply

Cisco is the world's largest supplier of transceiver modules and understands that any shortage of supply creates a painful ripple effect that propagates through to our customers and their customers. To ensure a stable supply base, we engage multiple suppliers and continuously monitor their strength and viability. We do the same for critical sub-component suppliers as well. Due to the highly granular nature of the optical component industry, lasers, photodiodes, and their respective packaging can be limited to a few sources. Therefore, it is important to manage that critical path.

Diversity of manufacturing sites is also a priority, as many optical component manufacturers set up production lines in the same handful of locations. The fruits of Cisco's supply strategy were evident in 2011 when optical component manufacturing capacity was hit hard by both the tragic earthquake in Japan and the devastating floods in Thailand. That they happened within the same year compounded the problem dramatically. While most of the optical component industry experienced shortages that continued well into 2012, our strategy of multiple suppliers and multiple manufacturing sites allowed customers to continue operations with almost no impact. In the end, only two transceiver products (out of hundreds) were on extended lead time.

Cisco also manages all of the PCNs that are generated by the suppliers that relate to change of manufacturing

site, sub-component change/EoL etc. We qualify the new version across all Cisco hosts as necessitated by the change. This ensures continuity of supply and lifetime product lifecycle management to our customers.

Our ongoing reliability testing (ORT) programs monitor production lines by randomly selecting samples and putting them through environmental stress testing. ORT helps to make sure that processes and materials continue as originally specified. Any gradual degradation can be detected early and corrective action can be taken before any field issue occurs.

Cisco Service

SmartNet is the final step in the comprehensive strategy to minimize risk to the customer. The qualification process and ongoing reliability testing minimize the incident rate of any technical issues. If anything does happen or if there are questions from the field on applications, SmartNet provides coverage.

Customers need only call Cisco's Technical Assistance Center (TAC) for help with debugging a problem whether it is caused by the Cisco host or the Cisco transceiver module. SmartNet service is not available to third party transceivers.

Case Studies

Some of Cisco's customers have experienced firsthand the pitfalls of using third party optics. Below are two such cases involving painful recovery activities.

- Case A. Cisco's Customer A is a $100B worldwide leader in telecommunication services. As a Tier 1 service provider, "5 nines" reliability is key to their strategy and brand. In 2008, Customer A purchased 500 units of third party transceivers for use with Cisco routers.

  After basic material incoming inspection, they found that the products did not meet their specifications. In order to avoid network downtime at critical customer sites (hospitals, schools, financial institutions, etc.), this Customer A concluded that there was no valid business case for third party transceivers.

- Case B. Cisco's Customer B is a provider of intelligence and information for businesses and professionals with over $10B of annual revenue. Tools and services are designed specifically to support financial, healthcare, legal, media, science, tax and accounting vertical industries. This customer uses a mix of Cisco switches and small routers.

  Upon investigation of a service disrupting incident, Cisco's Technical Assistance Center (TAC) discovered the presence of suspicious pluggable transceivers in Customer B's network. These transceivers were sourced from a Cisco-approved Gold partner and assumed to be genuine Cisco parts. Further analysis of over 11,000 transceiver ports uncovered more than 3,500 transceivers which were not genuine Cisco devices. Total network downtime resulted in a loss of revenue estimated to be in the $1M to $10M range.

Myths

Myth 1: Transceiver modules are standardized; therefore, they're all the same.

Even though IEEE specifies many of the protocols used, and MSAs define form factors and electrical interfaces, there is still quite a bit of room for variation. During qualification, we have encountered modules that get stuck in the port, contain incorrect firmware code, and exhibit link-flap and data errors, to name a few. Designs and manufacturing processes are, of course, corrected before releasing the product. Many of the problems observed are system-dependent and cannot be discovered by testing the module by itself.

Myth 2: As long as the module is qualified by its manufacturer, it should work on any platform.

Since module manufacturers do not test on Cisco or any platforms, there is no way to catch system-dependent issues. Problems that we haves observed include modules getting stuck in the port, modules not coming up, link-flap and intermittent data errors. See Table 1 for more detailed descriptions.

Even if a module is advertised as compliant with IEEE and MSA standards, only Cisco can verify specifications and functionality when used in Cisco switches and routers.

Myth 3: Cisco outsources to manufacturer X. Therefore, if I buy directly from X, then I am getting exactly the same product.

While it is true that Cisco works closely with other manufacturers, any genuine Cisco product is only available through Cisco or our approved channels. If a manufacturer supports both Cisco and its own

For More Information

Transceiver Module Group
https://www.cisco.com/c/en/us/solutions/service-provider/innovation/optics.html

branded modules, the product lines can diverge for a number of reasons. For example, Cisco's specification is often more stringent than that of the broader market. This could require a different component, different circuit design, or the product may be binned for certain quality metrics, such as eye-mask tests.

Another way for differences to arise is if a product undergoes a version change. If the change is not aligned with Cisco performance and system requirements, then we will not approve it. The opposite may happen as well. Cisco may require design iterations which the manufacturer does not apply to broader market product. In either case, two manufacturing lines may result.

Myth 4: Cisco SmartNet service contract only covers transceiver modules in Cisco hosts.

With Cisco's SmartNet service, customers can rely on Cisco TAC for technical support. TAC can help debug issues and replace parts if faulty. Cisco TAC is ready and able to diagnose and troubleshoot optics even when plugged into non-Cisco hosts.

Conclusion

There is indeed a difference between Cisco and third party transceiver modules. Cisco invests heavily in personnel and capital equipment for system-level testing and supply chain management. This ensures that customers experience minimal field issues on Cisco platforms. Furthermore, complete technical support and same day replacements are available if an issue does occur. Our acute focus on minimizing risks is a comprehensive benefit enjoyed by all of our optics customers.