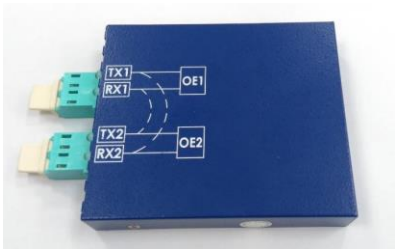
Optical Bypass Devices *Application Notes*

This application note introduces what Optical Bypass Devices are and provides examples of how they can be used to improve network availability and uptime. Formerica's Optical Bypass Devices (OBD) offering consists of Optical Bypass Modules (OBM) and Optical Bypass Networks (OBN), which are modules pre-integrated with Intel based Network Interface Cards (NIC) (see Figure 1). Optical Bypass Devices enable networks to be more resilient against unplanned failures by activating and providing network connectivity during host device/network appliance failures.

Figure 1. Optical Bypass Module and Optical Bypass Network



Optical Bypass Module: 2 port, LC Connector

Optical Bypass Network

There are three types of OBMs: passive, managed, and intelligent.

A passive OBM is integrated with industrial switch and automatically activates when the host device encounters a power failure.

A managed OBM has firmware and a built-in watchdog timer that listens for a ping signal from the host device, for example, an industrial PC. In the absence of that ping signal from the host device in a predetermined time, the OBM activates to ensure continued connectivity to the network.

An intelligent OBM is the most complex and integrates application logic of the host device into its function. It has a heart-beat monitor built-in and detects when the host device, i.e. network appliance, is compromised and functioning incorrectly.

Formerica Headquarters
5F-11, No.38, Taiyuan St., Zhubei City
Hsinchu, County 30265, Taiwan(R.O.C)
Tel: +886-3-5600286
inquiry@formericaoe.com

Formerica North America
Peter Liu
Cell: +1 408 667 4860
peter.liu@formericaoe.com
www.formericaoe.com

Figure 2 illustrates how managed Optical Bypass Device operates in normal mode and bypass mode, activating when network appliance fails to restore network connectivity.

Normal Mode:

- Network Appliance: Online & Functional
- OBM receives pings from Watchdog Timer and stands by
- TRX1 & TRX2 works independently
- Traffic directed to/from all appliances

Bypass Mode:

- Network Appliance: Offline
- No pings from Watchdog Timer
- OBM activates, latches TRX1 & TRX2
- Failed appliance bypassed
- Connection to remaining appliances restored

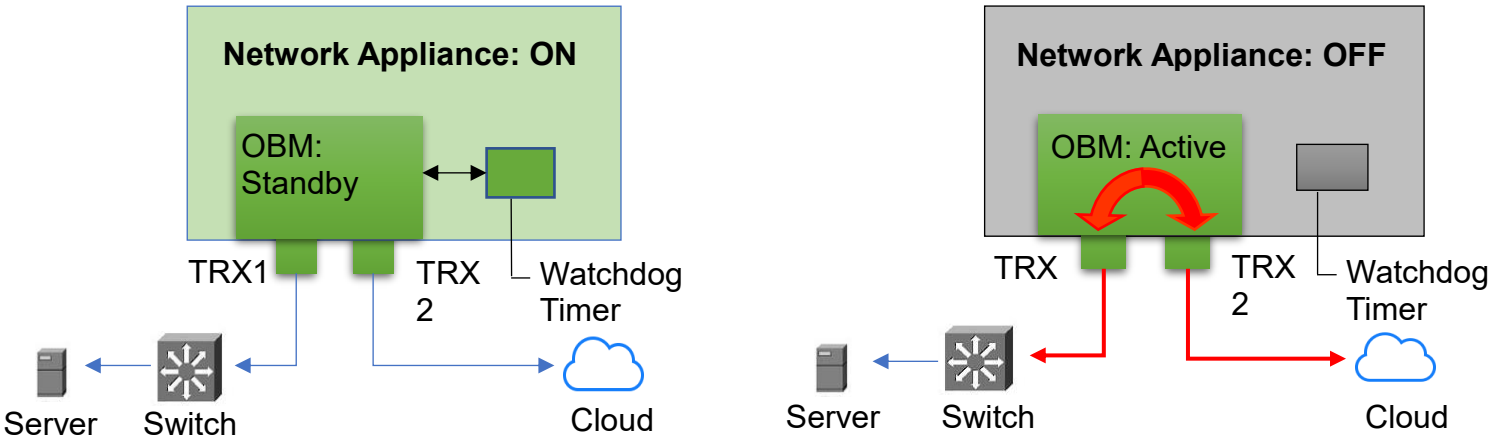


Figure 2. Optical Bypass Device protecting activating and restores network from interruption

Real-world case studies illustrate how Optical Bypass Devices provide critical function to improve network availability, connectivity and reliability.

Two parallel streets have daisy-chained traffic light controllers: the first does not utilize OBD and the second does. On the first street, when one traffic light controller fails, the traffic lights malfunction at that intersection and subsequent traffic light controllers downstream from the first failed controllers are also knocked offline. Due to domino effect, subsequent intersections all have malfunctioning traffic lights.

The second street has Optical Bypass Device installed on each traffic light controller. When one traffic light controller fails, the OBD activates to bridge the network gap so control signals continue upstream and downstream over the failed controller, restoring the integrity of the daisy-chained traffic controller network and only one intersection has malfunctioning traffic light.

Formerica Headquarters
5F-11, No.38, Taiyuan St., Zhubei City
Hsinchu, County 30265, Taiwan(R.O.C)
Tel: +886-3-5600286
inquiry@formericaoe.com

Formerica North America
Peter Liu
Cell: +1 408 667 4860
peter.liu@formericaoe.com
www.formericaoe.com

In a daisy-chain or a ring network topology, Optical Bypass Devises ensure network connectivity and availability by preventing failures from cascading down the chain or rest of the ring and stopping the domino effect. See figure 3.

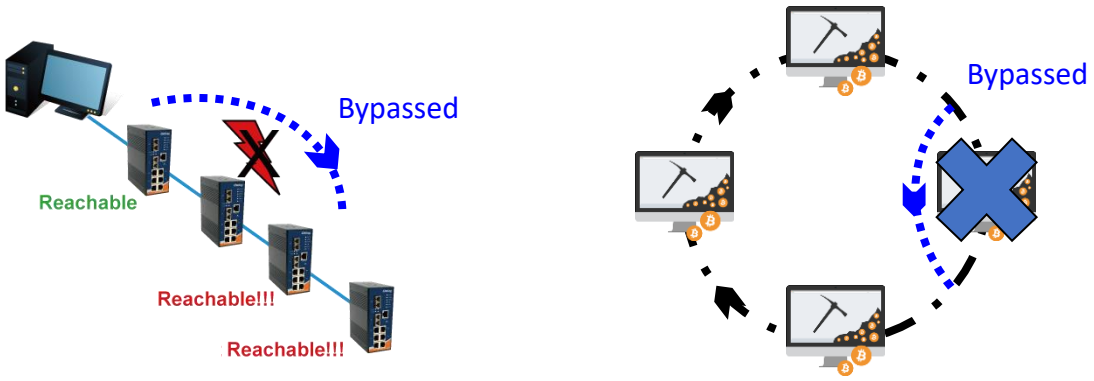


Figure 3. Examples of Optical Bypass Devices activating and reconnecting networks

An intelligent Optical Bypass Device can be integrated into DPI (Deep Packet Inspection) as part of IDS (Intrusion Detection System) and IPS (Intrusion Protection System). In the event the network appliance remains powered but sends out nonlogical data, the OBD activates and isolates the network appliance from the network until it can be examined or repaired. For example, an email server behaves maliciously by sending massive traffic to a specific domain may be hacked and participating in a DDoS attack. When the intelligent OBD detects this, it activates and isolates the compromised server from the rest of the network until the server can be examined, thereby limiting the extend and damage of the intrusion into the network.

In addition to DPI/IPS/IDS and traffic signal relays application, Optical Bypass Devices can be used in myriad application such as parking garage systems, bitcoin servers, etc. It is an essential device to stop failures from cascading in a daisy-chain or ring network, or to isolate an problem node from the network. It improves connectivity and availability of the network when problems occur and is essential to modern network design.

Optical Bypass Devices are available in 4 data rates: 1G, 10G, 40G, and 100G. Options include 2 or 4 ports, as well LC or MPO connectors. They are available as modules or pre-integrated on Intel based NICs.

For more information, please contact Formerica Optoelectronics.

Formerica Headquarters
5F-11, No.38, Taiyuan St., Zhubei City
Hsinchu, County 30265, Taiwan(R.O.C)
Tel: +886-3-5600286
inquiry@formericaoe.com

Formerica North America
Peter Liu
Cell: +1 408 667 4860
peter.liu@formericaoe.com
www.formericaoe.com