OWL Cyber Defense

High Availability

Maximize Uptime & Prevent Data Loss

USE CASES

- Loss of power
- Network outages
- Maintenance updates

SUPPORTED PROTOCOLS & DATA TYPES

- Aveva PI System (OSIsoft)
- E-mail
- FTP
- MQTT
- OPC Classic (DA/A&E)
- RFTS
- SFTP
- SNMP
- Syslog
- TCP/IP
- UDP (Unicast, Multicast)

High Availability for Maximum Uptime

For organizations who cannot risk downtime, a high availability solution can provide 24/7/365 protection and communications. The utilization of data diodes to enable one-way transfers of data from OT to IT is an industry proven way to ensure access to data while preventing OT environments from being attacked. A single data diode is sufficient when certain durations of downtime can be tolerated during maintenance updates or outages. However, when access to data is mission critical, high availability data diode solutions maximize uptime and ensure that data never stops flowing during a hardware or network outage. Owl's Perimeter Defense High Availability Solution (OPDS-HA) ensures maximum uptime with no data loss when outages and network interruptions occur.

Prevent Data Loss During Network Outages

OPDS-HA consists of a pair of OPDS data diodes to create a high availability solution and provides unmatched flexible protocol and datatype support, eliminating many of the challenges associated with deploying data diodes in high availability environments. The high availability failover allows customers to maintain operational data flows whether there are planned (maintenance updates) or unplanned (communication disruptions) outages.

High Availability vs Warm & Cold Standbys

High availability can mean something different to everyone. Some think of high availability as warm and cold standbys. While warm and cold standbys can be inexpensive and flexible, organizations can experience long downtimes, require manual intervention to swap cables and switch to operational mode, and can have significant data loss. However, with the OPDS-HA solution, organizations can experience failover in near real time, no data loss, and no manual intervention.
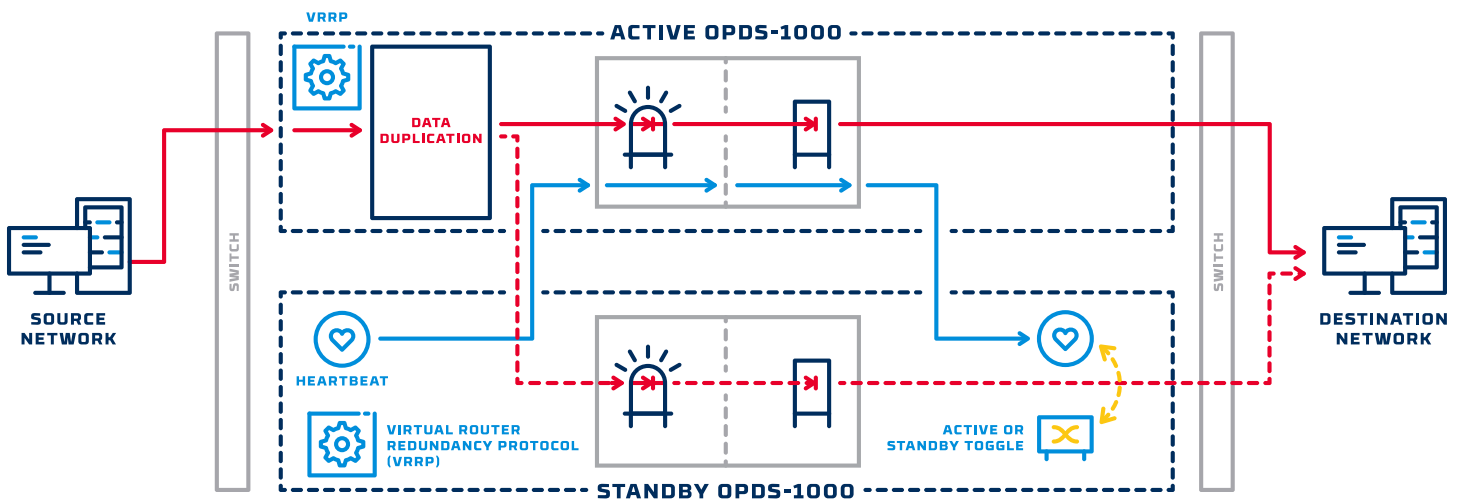
How OPDS-HA Works

The OPDS-HA solution deploys a pair of OPDS-1000 to create a high availability cluster. Virtual Router Redundancy Protocol (VRRP) software runs on the Source side of the each OPDS. It provides for transparent failover and eliminates the single point of failure in the static routed environment. VRRP assigns an Active and Standby Node within the High Availability cluster. Network traffic passes via the Active Node. Data is duplicated and transmitted across the Active and Standby Data Diodes. UDP heartbeats manage de-duplication of data. In the event that there is an Active Node failure, the Standby Node becomes Active.

The Standby Node passes traffic until the original Active Node resumes operation.

UDP Heartbeats are sent from the Standby Source Node over the Active Source Node to the Standby Destination Node. This verifies the operational status of each Node including:

- Standby Source Node
- Active Source Node
- Owl Data Diode link between Active Source Node and Active Destination Node
- Active Destination Node
- Standby Destination Node

When the UDP heartbeat arrives at the Destination Standby Node, the Active Node is deemed fully operational. When heartbeats are available in the Standby Destination Node, the Standby Destination Node toggles into maintenance mode, stopping all traffic, avoiding data duplication. When heartbeats cannot be detected by the Standby Destination Node within a specified time period, the system toggles out of maintenance mode and the Standby assumes Active status.