Providing Network Connectivity to Intelligent rPDUs Without Requiring Expensive Switch Ports for Each

A Vertiv Application Brief

Benefits

Cost Effective

Redundant

Reliable

Challenge

Current rPDUs need to be replaced with intelligent rPDUs within cabinets. Each intelligent rPDU needs a network connection. Current network switches are close to capacity. Implementing both new network switches and new intelligent rPDUs would be cost prohibitive.

Application

Three possible applications are to use a network port for each rPDU, daisy chain the rPDUs or daisy chain the rPDUs with redundant network connectivity.

Solution

The Vertiv Geist Upgradeable (GU) rPDU daisy chain application provides redundancy by offering a fault-tolerant daisy chained solution utilizing Rapid Spanning Tree Protocol (RSTP) which allows users to connect multiple rPDUs to the network while only using two network switch ports.

A data center needs to introduce power and environmental monitoring at the cabinet level. The current rPDUs need to be replaced with intelligent rPDUs within data center cabinets. Intelligent rPDUs require a network connection each which means that the network switch needs to have capacity for the additions. However, the network switches are almost at capacity and adding additional switches is expensive. There are budgetary constraints that prevent replacing both the rack PDUs and adding new network switches.

Terminology

Rapid Spanning Tree Protocol (RSTP)

RSTP is a network protocol that creates a logical loop-free topology for Ethernet networks. It prevents bridge loops and the broadcast radiation that results from them. RSTP allows a network design to include spare, or redundant, links to provide automatic backup paths if an active link fails. This is done without the danger of bridge loops or the need for manual enabling or disabling of these backup links.[1]

Fault Tolerant Connection

A fault-tolerant connection utilizes a combination of hardware and software technologies to redirect network traffic if a link or single device is down ensuring that all other devices on the network loop remain accessible.

HOW CAN I PROVIDE RELIABLE NETWORK CONNECTIVITY TO ALL INTELLIGENT PDUS WITHOUT REQUIRING EXPENSIVE SWITCH PORTS FOR EACH?

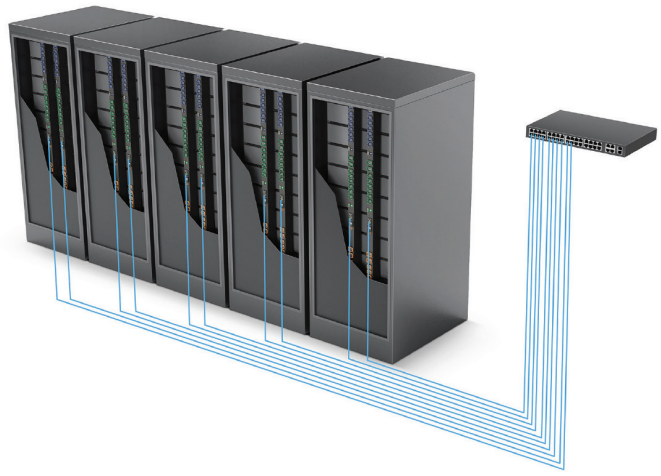
[1]LAN/MAN Standards Committee of the IEEE Computer Society, ed. (2004). ANSI/IEEE Std 802.1D - 2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges. IEEE.

Providing Network Connectivity to Intelligent rPDUs Without Requiring Expensive Switch Ports for Each

A Vertiv Application Brief

1. Traditional Connections: A Network Port for Each rPDU

Traditionally, each intelligent rPDU in a rack would require the use of one port on a network switch. The cost associated with providing a network connection to each rPDU can be hundreds of dollars. Furthermore, if the addition of intelligent rPDUs was not proactively planned for, the network switch may be at or near capacity leaving few options for connecting rack PDUs without adding costly network switches.



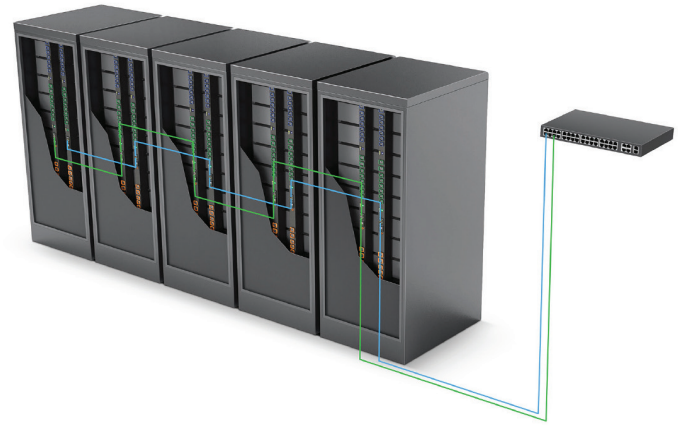
PROS	CONS
Each Intelligent rPDU has dedicated network connectivity.	• Expensive • Makes Expansions Difficult • Time Consuming and Costly

2. Daisy Chaining

In a standard daisy-chain application each rPDU is connected to the next in line using a patch cable and each rPDU requires an IP address. While this method can significantly reduce the number of switch ports used, it also reduces visibility if the chain loses power.

Another method for daisy-chain application is a Master/Satellite. This option has a main host device that additional rPDUs connect to (typically 1-4 satellites, possibly more). The host collects the data from the satellite rPDUs and provides a single interface. Once again, this option reduces the number of switch ports used, but causes major redundancy issues if one rPDU in the chain loses power or a cable is disconnected.

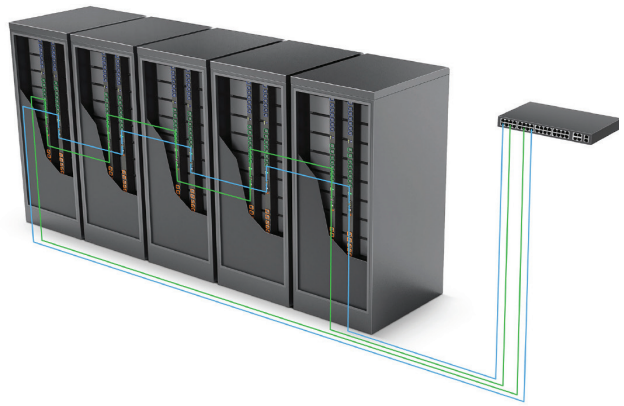
A third daisy chain option is to connect all rPDUs in the same rack to a single network port. In this scenario, if the first rPDU were to lose power or if the monitoring card fails, the user could lose visibility to the entire cabinet.



PROS	CONS
Each intelligent rPDU has network connectivity and only uses a single network switch port.	Single point of failure for network connectivity to all rPDUs in a rack.

3. Daisy Chaining with Redundant Network Connectivity

The third option uses network loops and Rapid Spanning Tree Protocol (RSTP) to provide a redundant communication layer that is not available with standard daisy-chaining. As with the previous option, rPDUs are connected in a daisy chain fashion; however, with this option the final rPDU in the chain is connected back to the switch. Normally loops are not implemented because they cause 'broadcast storms' which result in network failure. RSTP was developed to address this issue, therefore making network loops a plausible solution. RSTP prevents the network loop from causing major communication failures that would otherwise occur. With loops and RSTP, there is no longer a single point of failure; instead there is a redundant network connection to each intelligent rPDU.



PROS	CONS
• Cost Effective • Each Intelligent PDU has Network Connectivity Configuration • Provides Redundancy	RSTP may require additional network or switch configuration.

Solution

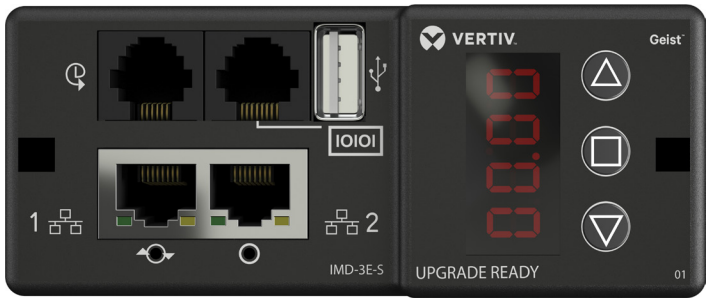
The Geist daisy chain application provides redundancy by offering a fault-tolerant daisy chained solution utilizing Rapid Spanning Tree Protocol (RSTP) which allows users to connect multiple rPDUs to the network while only using two network switch ports.[2]

Geist Upgradeable (GU) rPDUs[3] have two available network connection ports and implement RSTP. The daisy chain configuration uses both GU rPDU network ports to create an Ethernet ring connection from one end of the rack row to the other. The end of the chain loops back to the network switch to create a fault tolerant connection.

The fault-tolerant connection utilizes a combination of hardware and software technologies to redirect network traffic if a link or single device is down. This ensures that all other devices on the network loop remain accessible.

RSTP allows for up to 40 devices per network loop, including switches. The GU rPDU is programmed to allow 40 devices (typically two network switches and 38 rPDUs). However, if the network switch has been configured to allow less units that could take priority. A network administrator will want to review the configuration of RSTP enabled switches to make sure they are configured to allow the desired loop size.

Using Geist Upgradeable rPDUs fault-tolerant daisy-chaining reduces the cost and complexity of adding intelligent rPDUs to the data center.



[2]While it is possible to connect all the rPDUs in one daisy chain, Geist recommends using separate daisy chains for A and B rPDUs to improve redundancy in the event of an A or B feed power failure.

[3]While Geist products are capable of providing a network port for each intelligent rPDU it is not the recommended solution in regards to a cost effective solution.

Vertiv.com | **Vertiv Headquarters,** 1050 Dearborn Drive, Columbus, OH, 43085, USA

SL-70489 (R06/19)