

MEDIA FOR



IPLM: Why it achieves value beyond port count

Intelligent Physical Layer Management systems can bring to the physical layer the capabilities that are possible at higher layers of the network.

by Michael Pula

Achieving maximum network uptime to run mission-critical applications requires attention to all aspects of good network housekeeping. With links in the data center numbering in the thousands, and with the density of connected devices becoming more difficult to physically trace, this good-housekeeping effort includes a view into physical layer connectivity. Of all network layers, however, the physical layer typically offers the least amount of visibility.



Good network housekeeping goes beyond proper cable management to include the ability to electronically monitor or redirect links, keeping the cable infrastructure intact

Intelligent physical layer management (IPLM) systems provide this visibility. These systems map, monitor, and manage real-time patch-field connectivity, and continuously record networked asset movements and configuration changes occurring throughout the enterprise and data center.

Automating real-time information

The core value these systems bring to an organization is automating the process of gathering and

recording accurate, real-time information on the status of connections across the network, thus minimizing downtime and improving operational efficiencies. IPLM systems are being used for more than just monitoring of ports and cords, and are adding additional value by helping network managers optimize network capacity, improve asset tracking, and enhance network security.

Traditional network management systems, covering OSI Layer 3 and higher, monitor multiple network and data traffic parameters. These solutions typically identify that a broken or interrupted link has occurred, but do not report on the precise physical-layer connections where many problems are known to originate. The process of physically locating or tracing the links may take an hour or more to accomplish.

In contrast, the focus of an IPLM tool is to guide network administrators in planning and implementing cabling changes, and to provide real-time monitoring of patch-field connectivity events. An “event” with the physical layer is defined as a change in state of the patch field or monitored links (i.e., a connection or disconnection of any link or network asset).

To accomplish these tasks, IPLM systems rely on three specific functions:

- *Intelligent patch fields* and/or cords provide real-time connectivity information, which is read by the active hardware;
- *Active hardware* scans or monitors the patch field and reports changes in state;
- A *software application* compiles the information, stores it in a database, and may formulate a recommendation or response based upon system conditions, such as pending work orders.

These functions work together to track and record all network events in real time, ensuring that the network database is current and accurate. As activities are recorded to the database, the system analyzes this information and takes appropriate pre-programmed actions. For instance, in a data center, an unscheduled disruption or alteration to a server connection might trigger an alarm to a network administrator. Because the location and port number of the event are readily available, IT or security staff can quickly locate and efficiently react to this and other unauthorized network changes.



Panduit's PanView IPLM System uses light-emitting diodes (LEDs) integrated into the patch panel to guide changes to network connectivity. A blinking LED indicates that a patch cord needs to be removed, while a steady LED indicates where the patch cord needs to be inserted.

Many IPLM systems integrate with other managed network systems to enable greater control of the entire network. By extending traditional network management of OSI Layers 3 and above into the physical layer (Layer 1), organizations can monitor all devices in the network with greater visibility.

IPLM systems also improve the efficiency and accuracy of moves, adds, and changes (MACs) through a work-order process that helps network managers plan, prioritize, and assign all changes in the system. As the MACs are being completed, the system records the time and date of the actions, and automatically updates the database to reflect the new patch configuration, ensuring that patch-field information is 100% accurate at all times.

These automated processes reduce mean-time-to-repair (MTTR) by helping prevent human error and unauthorized patch-field changes, whether deliberate or accidental. In this way, network managers can leverage the IPLM tools to streamline operations and maintenance processes, resulting in lower technical-service costs and increased network uptime and reliability. Furthermore, network maintenance can be directed remotely from a network-management station and assigned to specific individuals.

Asset management is a largely overlooked aspect of organizational networks. In fact, Gartner Research (www.gartner.com) found that even with network-management tools in place, organizations fail to track 40% of their distributed- computing hardware assets. Failing to account for all networked assets can negatively affect network manageability, cause delays in MAC processes, and even impact the reliability of service levels. This can introduce a multitude of business risks-operational, financial, legal, and regulatory.

What's connected where?

To mitigate these risks, IPLM technologies can identify and track the movements of all assets connected to the network, giving administrators the ability to see what is connected and where. These systems identify new assets connected to the network as well as existing assets that have not been used for a prescribed period of time. Also, if the database is unable to locate a given asset at its expected location, the network manager can be alerted to determine whether the asset is missing or is actually present but disconnected/powered off. This feature of IPLM systems helps to prevent potential device theft or unauthorized device relocation.

Using Simple Network Management Protocol (SNMP) on connected devices-which may include wireless access points, Internet Protocol surveillance cameras, or even a laptop connected to the network-the IPLM system can query the network infrastructure for specific information on these devices, such as type, and IP and MAC (media access control-not to be confused with moves/adds/changes MACs) addresses. Furthermore, an IPLM system can document and record any movements to a centralized database, providing real-time updates of changes while ensuring that information is accurate at all times.

For example, before an individual logs onto, or attempts to log onto, the network with a laptop, the system can identify the laptop via its MAC address and the location of the laptop within the network. By monitoring the laptop's physical connectivity, the organization continually verifies that the laptop is on-site and is active, aiding in hardware asset management. This visibility can be extended to any endpoint device that is connected to the network, including Voice over IP phones and IP security cameras, as well as hardware such as servers.

The ability of IPLM solutions to map all physical connections also enables network administrators to optimize data center capacity by tracking switch-port availability in the database. IPLM systems can feature management software that graphically displays tracked assets within the network, providing a virtual map of servers and other active data center equipment as well as the connectivity between the equipment. IPLM tools can also be used to monitor port consumption and notify network managers as

the network approaches capacity limitations, as well as identify where available network ports and assets are located to quickly reclaim network capacity. (See sidebar, "IPLM in action," page 34.)

Security at and beyond the physical layer

Intrusion detection is "top of mind" for many IT managers and corporate security personnel. Security in the data center has traditionally centered on preventative measures, such as restricting unauthorized access to the network via login/password, domain, subnet, virtual private network, or other similar restrictions to protect the network from data corruption, viruses, or actual physical damage. Security of telecommunications rooms can also be enhanced through use of electronic locks, badge readers, and other lockout technologies, but these measures cannot prevent employees or visitors within the building from gaining network access.

With an IPLM system, unauthorized network access can be identified in real time by comparing the MAC and IP addresses of devices requesting access to those authorized within the network database. Upon connection, any unidentified MAC or IP addresses would trigger an alert to IT or security personnel so that immediate action can be taken, helping to prevent potential security breaches and minimize costly network downtime.

Detecting an intrusion and triggering an alert is only the beginning. Integrating an IPLM system into a comprehensive managed network system can allow preprogrammed security actions to be automatically triggered within the network. For instance, upon detection of an unauthorized network access attempt, the IPLM system can trigger the managed network system to immediately close down the port or site of the attempted access. Additionally, this event could initiate another function, such as the dispatch of security personnel to the location of the attempted breach.

Security has also expanded beyond these critical issues to include such concepts as regulatory compliance and reporting requirements. Through a combination of static inventoried demarcation points and active monitoring of asset movement through the network, IPLM systems automate physical layer documentation to ensure that sensitive information is recorded accurately and securely. These systems help organizations comply with industry regulations, such as Sarbanes-Oxley, HIPAA, and the Gramm-Leach-Bliley Act (GLB) with comprehensive reporting that reduces the costs associated with preparation for regulatory audits.

In situations in which data warehousing protects critical information, the ability to restore the physical infrastructure links that access data is just as important as the ability to restore the content itself. IPLM systems can assist in the process of recovering data center and LAN configuration information; as the system monitors the physical layer, its database continuously records asset movements and configuration changes occurring throughout the system, eliminating the need for manual record-keeping. The database information may also be used to provide a "snapshot" of the enterprise network, guiding the re-creation and restoration of all connectivity points throughout the network, including the data center and all data rooms, as part of an emergency or disaster-recovery measure.

The security and availability of network-based processes are critical to the business health of most enterprises. IPLM solutions address these concerns by providing additional physical layer visibility via continuous monitoring of the patch-field connectivity, as well as documenting and reporting all physical-layer events. This visibility lets network managers quickly respond to disturbances in the network, minimizing downtime and improving security. IPLM systems also enable network managers to conduct maintenance from remote locations, for more-efficient management of network resources and

substantially reduced operational costs.

Tracking assets, mapping connections

IPLM tools provide additional value by enabling asset tracking and resource optimization across increasingly complex network architectures. The ability of IPLM tools to track asset movements enhances security by helping network administrators quickly identify unauthorized devices and facilitate the access of authorized users. These tools also help IT staff optimize network capacity by mapping all available physical connections and monitoring port consumption.

For organizations searching for optimum availability, security, and manageability of their physical infrastructure, an IPLM system is a critical solution that enables both operational efficiencies and cost savings.

MICHAEL PULA is product line manager with Panduit Corp. (www.panduit.com).

IPLM in action

Defiance Electric and Crossover Inc. of Enfield, NH (www.defianceelectric.com) has provided design/build services to commercial, industrial, and institutional customers since 1978. Pete Hadlock, vice president, says, "Panduit has worked with Defiance Electric and Crossover Inc. to establish the kind of cooperative partnership that we can deliver to our own clients."

Recently, Defiance specified Panduit's PanView System, an intelligent physical layer management system, to a client seeking efficient remote network-monitoring capabilities to reduce operating expenses and optimize overall network reliability. Even though the client understood the benefits that the PanView System offered to remotely manage patch fields, the client was surprised how quickly the system helped optimize its network investment.

In one telling example, the client needed additional port space and inquired about purchasing new switching equipment. As an alternative, Defiance Electric and Crossover Inc. recommended using the PanView System to run a report of assets to quickly locate any "forgotten" network ports. Sure enough, the report revealed a port that had not been used for more than 90 days. The client simply reallocated this port, leveraging assets it already owned and avoiding the cost of new network equipment and cable drops.

The entire process, from the initial phone call to the identification of the port, took less than 10 minutes.-
MP

Cabling Installation & Maintenance September, 2007

Author(s) : Michael Pula

Find this article at:

http://cim.pennnet.com/display_article/305136/27/ARTCL/none/none/IPLM:-Why-it-achieves-value-beyond-port-count