

Intelligence at the Physical Layer

Smart Cabling — Better Security

Any network manager will tell you the importance of a fully documented network. This documentation should include all workstations, IP addresses, router configurations, firewall parameters, etc. But this documentation may fall short at the physical layer. In particular, older networks that have gone through many Moves, Adds and Changes (MAC work) are not likely to have current documentation. In real time – during a crisis, this can mean the difference between quickly solving and wasting precious time locating the source of the problem

Perhaps the best illustration is an example taken from a customer that had an issue with a errant device on the network. To provide some background, the company had 5 buildings in the campus. A laptop was creating a denial of service attack from the inside due to a virus. The switch would shut down the port, IT would go to the telecommunications area to determine the location of the misbehaving device. But when IT got to the physical location of the switch, the physical layer (largely undocumented) became an issue – because short of tracing the cable, there was no way to find the location of the laptop. They began tracing the cables only to find that the laptop was no longer there. The laptop user felt that his loss of connectivity was due to a problem with the network. Each time he was disconnected, he moved to another location only to find that after a period of time, he would quickly lose his connection again.

In this scenario, the switches were doing their job by shutting down his port. The user was troubleshooting his own problems. IT was having trouble finding him to correct the problem... and the cycle continued. At one point, the user decided that it must have something to do with the equipment on that particular floor, and moved to another floor. After being disconnected again, he decided that it must be security settings for that building. He then moved to another building. And again, the cycle continued. Roughly 5 hours later, the laptop and user were found and the problems were corrected. For the IT staff, this was 5 hours of pure chaos! For the user, this was 5 hours of pure frustration.

In other scenarios, compliance and overall network security can also be compromised at the physical layer. Most companies have some desks and cubicles that are largely unoccupied and used by more transient staff members. Conference rooms with available ports can also pose a risk. In many vertical markets where compliance is required, these open ports can cause a company to fail their audits unless they are shut down completely or a means exists to allow only certain users can gain access to the network through these connections. The only other option is to firewall these ports from the actual network, which would mean a reconfiguration each time that an authorized network user wanted to utilize the port. All of these risks and their remedies can be burdensome to an IT manager.

In the data center and telecommunications areas, technicians provide an additional risk if they accidentally unplug something that should not be unplugged. Suppose the accidental disconnect was a VoIP switch or a critical server. What if a piece of equipment leaves a facility that contains critical information, as reported many times in the news recently? How does a network manager know who has accessed the network? Where did they access the network? How is access documented? And finally, how are moves, adds and changes managed?

THE INTELLIGENT ANSWER

Intelligent patching has been around for some time, however, the functionality has improved from the original releases. In any of the scenarios above, an intelligent infrastructure management system, such as Siemon's MapIT™ G2 would have allowed the network manager to right click on the offending device, view the entire channel and even locate the device on a graphical map. (See Figure 1).

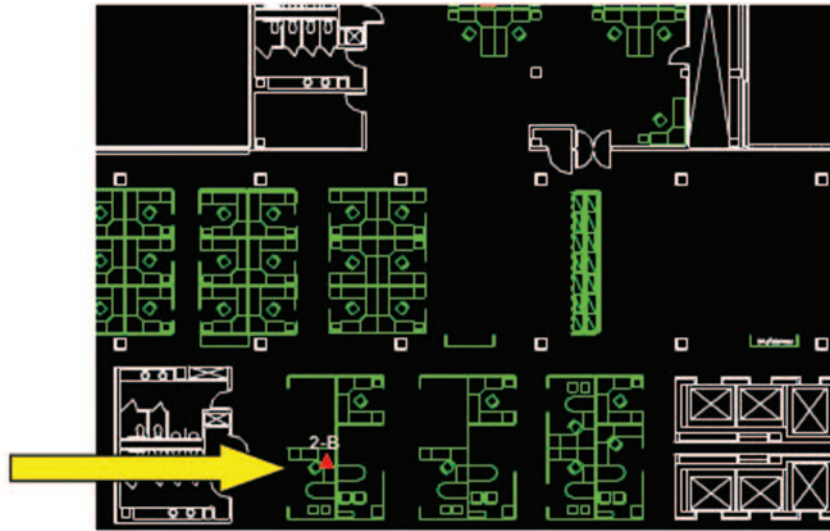


Figure 1: Graphical Layout of Building With Outlet Locations

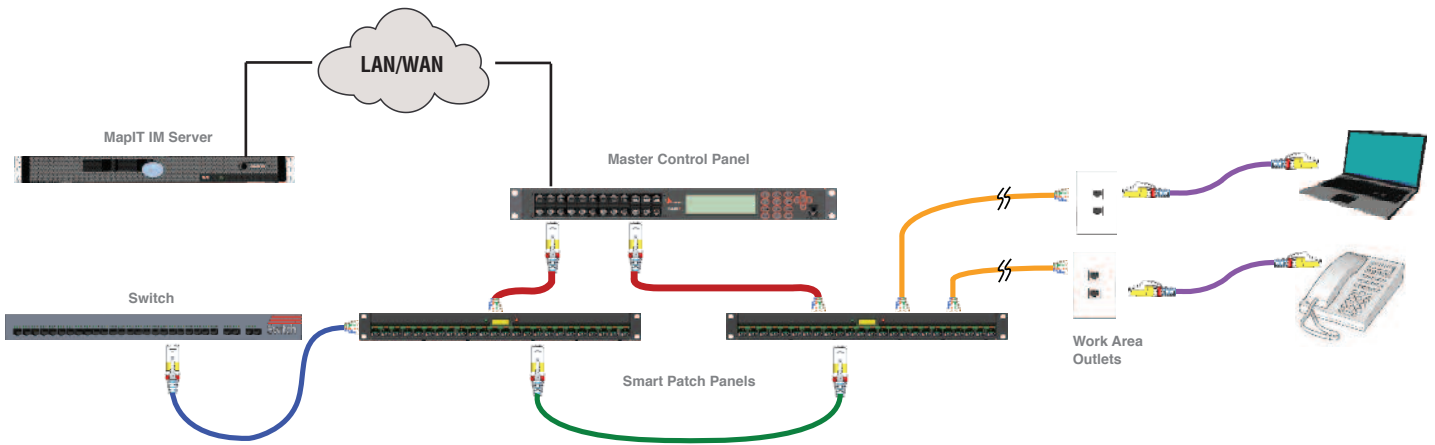
In the figure above, you will notice that the outlet location is clearly marked on the drawing. By adding the physical layer, network managers are no longer limited to upper layer information only. While knowing MAC address, IP address and logon information is certainly helpful, should physical layer documentation be out of sync with the actual infrastructure, finding problem devices can be a daunting. MapIT™ G2 intelligent patching bridges that gap.

HOW THE SYSTEM WORKS

The system works through a combination of sensor-enabled hardware and software. On the hardware side, MapIT G2 smart patch panels and fiber enclosures are configured with a sensor pad above each port. MapIT G2 patch cords and jumpers have a standard RJ45 interface or a standard fiber connector, and includes a "9th conductor" and contact pin designed to engage the sensor pad. This additional connection allows the system to detect any physical-layer changes in real time. This info is first processed in the smart panels and fiber enclosures and displayed in an on-board graphic LCD for patch cord tracing, diagnostics and technician guidance. A single, twisted-pair cable channel connects the smart panel to a 1U MapIT G2 Master Control Panel, which can monitor up to 2880 ports, relaying the information to the central database running MapIT Im software.

The software is purchased on a per port basis and is written to work either as a standalone application, or can be integrated with an existing network management package. In an integrated configuration, a device and its channel can be traced from within a network management package such as HP OpenView. A simple right click on the device and the MapIT IM software can be launched showing an immediate trace of the physical cable. The trace includes all the information about the channel including patch cords, where the channel terminates, the number of connectors in the channel, and can show the physical location of the device on a CAD drawing.

The software reads the object identification information for network devices through SNMP and can also send SNMP (including version 3) traps to shut down ports based on user defined parameters. This provides great benefit when the physical layer is included. For instance, if you wanted to know the location of every PC on your network that was running Windows 2000, you could have it displayed graphically as well as in report format.



The Virtual Wiring Closet (VWC) module provides documentation on the telecommunications rack including connectivity, patch cord length, where each device is connected, etc. It becomes a data dictionary for your racks and/or cabinets. The benefit of MapIT G2 is that it will track MAC work without having to update spreadsheets and documentation manually. It also includes a work order module for work order creation. Work orders can be dispatched, displayed onsite on smart panel displays and the changes made are automatically tracked, allowing a manager to know when the work was completed.

This can also be integrated with other security systems such as NetBotz® (owned by APC®) or video cameras. Based on user defined triggers, for instance when someone unplugs a VoIP switch, a camera can snap a picture, write it to the log, and as you would expect from management software, can provide alarms via email, cell, pager, complete with escalation for unanswered alarms. Contacts can be placed on doors to rooms, cabinets, etc. As soon as the contact is broken, the same logging can occur including a photo in the log indicating not only date and time, but additionally photographic/video evidence of the culprit.

While these are only a few of the benefits of MapIT G2, as one can see they are significant. If we go back to the examples at the beginning – in the campus scenario, a simple right click would have saved 5 hours of chasing down a user. Not only would the documentation be up to date, allowing the network manager to know where that switch port terminated in the building, it could also have shown this graphically. They very likely would have gotten to the user before his frustration started and he moved the first time.

Where security and compliance related issues are concerned, the additional documentation and logging abilities not only enhance a company's security position, but also answer many of the compliance related requirements of documentation and access logging. After all, most troubleshooting and investigations start with who, what, where, when, why and how. By adding the physical layer to your overall management the answers to these questions are much easier and more thorough.

For a demonstration of MapIT G2 intelligent patching that provides the full capabilities of the system, please contact your Simeon sales representative. Isn't it time to document and monitor **all** of your network?

The Americas
Watertown, Connecticut
Tel: (1) 866-548-5814 (US)
Tel: (1) 888-425-6165 (Canada)

Central & South America
Bogota, Columbia
Tel: (011) 571 317 2121

Europe/Middle East/Africa
Chertsey Surrey, England
Tel: (44) (0) 1932 571771

Asia Pacific
Shanghai, China
Tel: (86) 21 6390 6778

Japan
Tokyo, Japan
Tel: (81) 3 5437 1580