

INTELLIGENT INFRASTRUCTURE MANAGEMENT (IIM)

A quality patching system sits at the very heart of successful network management and when it is correctly specified, installed and maintained will ensure performance criteria are met. Ken Hodge, Chief Technology Officer at Brand-Rex identifies the different patching systems and explains how modern intelligent infrastructure management (IIM) can increase efficiency and save money.

There are a variety of methods to manage network connectivity and monitor moves, adds and changes (MACs). Poor network management and the use of non-compliant products can result in inefficiency, while failure to employ suitable processes and procedures can be highly detrimental to overall network performance.

Many and varied

A patching system that is not fit for purpose can jeopardise the smooth running of a network and result in extended periods of downtime. For network managers, knowing how the various parts of a system are connected provides an invaluable shortcut to problem solving.

The most basic type of patching 'system' is all too common in smaller businesses with few users and involves nothing more than a network manager making a mental note of what each patch cord is connected to. It relies on one person being able to identify any network failures or manage the small amount of MACs that might occur.

It is not difficult to see how this method could lead to problems if, for instance, that person should leave the company. With no documentation, a full audit would have to be carried out to ascertain how the network is connected.

The written word

Although most network managers will recognise the benefits of having written documentation, this often takes the form of a simple spreadsheet. If the various links and connections are all detailed, and providing any MACs are carefully logged, this should provide a reasonable record of how the network is configured. However, problems could easily arise if the master spreadsheet isn't updated or if any changes to the network are not noted, making the information worthless.

Variations on this theme usually involve the use of different coloured patch cords to represent a specific floor or department, which can help to find the cause of a particular problem.

Safe and secure

Solutions are now available which help keep the patch panel and patch cords free from malicious damage. Locks can protect an RJ-45 copper outlet or fibre adaptor by blocking cord access and preventing tampering, while a special key provides full access to other adjacent ports. By making removal of the patch cord impossible it can also help avoid accidental disconnection of the cord, which is particularly useful in public areas such as schools and hospitals.

Density is also important as minimising on-site installation time means saving money. Modern high density patch panels allow accessibility to cabling and use modularity to enhance operational flexibility. They facilitate patch cord routing directly into the rack vertical side management, thus increasing density and easing undue stresses on the cords.

Up to scratch

Despite the commonly held view that the humble patch cord is of little or no significance, nothing could be further from the truth. In fact, when it comes to ensuring network performance, it couldn't be more important.

Brand-Rex's own research into patch cord quality has found some truly shocking rates of non-compliance. A few years ago the company undertook tests on a number of commercially available Category 5e and Category 6 patch cords and found that over 75 per cent did not meet the TIA/EIA-568-B.2-1 standard. If these results are taken at face value it is clear that we are not dealing with a minor problem and other manufacturers have carried out tests since that time and obtained similar results.

Packet loss and slow running networks are just two consequences of using non-compliant patch cords. Installing a high quality product for the permanent link and then ruining the channel performance by using poor quality patch cords makes no sense and ultimately the price is paid with an inferior infrastructure.

Not only do many of these products fail to deliver the correct performance, they are unlikely to comply with BS EN50174-1:2009 which states that consideration should be given to cables having non-corrosive, fire retardant and low smoke/toxic emission properties.

To avoid any danger, when installing a system from Company X, play it safe and install Company X's patch cords. There may be cheaper patch cords out there, but as the old saying goes, 'you get what you pay for' and it's simply not worth taking the risk.

Smart thinking

For those seeking the ultimate in network monitoring, intelligent infrastructure management (IIM) is the answer. Since IIM was first introduced over a decade ago, it has become widely used in network intensive environments such as financial institutions, petroleum companies, disaster recovery sites, communications companies and data centres. In fact, any businesses that perform a large number of MACs, have immature processes, or which have multiple locations to manage, are good candidates for its adoption.

An IIM system will streamline documentation processes and substantially reduce the operational costs of network ownership. Asset management and utilisation can be drastically improved as it electronically detects and logs the physical location of all network assets, audits the equipment and creates an asset register. MACs are completed more quickly and easily and are therefore more cost effective.

IIM should also be considered by companies that as well as requiring greater control and visibility of their infrastructure, have to comply with Sarbanes-Oxley, Basel II and other regulatory requirements. It is also a highly complementary tool for organisations adopting best practices for process optimisation and service management. These disciplines include processes for configuration management, capacity management, change management and problem management.

Made to measure

IIM uses a combination of web-based software and intelligent hardware to maintain an accurate, real-time connectivity database of active equipment and physical layer components. These systems are designed to bring a traditionally inert network infrastructure under control and align it to the various management and diagnostic processes within the IT function. Doing this gives the end user an unprecedented level of visibility of an organisation's network assets, how they are connected together and where they are physically located.

IIM typically operates on a cross-connect topology and can be installed in Category 6 and 6A cabling systems, in either unshielded or shielded variants. Fibre options include all current standard fibre types with SC, LC and MPO connectivity.

Most IIM systems use an intelligent patch cord with a 9th wire between the panels in the wiring racks to manage and monitor connectivity. Patch panels are connected to a scanner system that sends and receives real-time connectivity information to and from the SP4E management station. In some situations, it is also possible to retrofit certain IIM systems into a legacy non-intelligent network.

All inclusive

When they first entered the market IIM systems were seen as the preserve of larger networks, due to the cost of purchase and implementation. However, there are now systems available that can suit the needs of businesses of all sizes.

At one end of the spectrum are state-of-the-art software based systems that have a client/server application on top of an SQL relational database. These work via standard SNMP with a network topology of intelligent hardware in order to control, map and monitor both the physical layer and active LAN equipment. They include features which track end-to-end network connectivity from PCs, telephones, IP phones, printers etc. through the connecting hardware, to the network equipment.

However, not every end user requires this level of functionality and at the other end of the spectrum are IIM systems that offer the key elements of a traditional enterprise monitoring system without the complexity and require no additional software or servers.

These systems collect information from patch panels and communications racks and detect any changes in connectivity. They then notify designated staff who can then access specific details from a permission based GUI via a web browser. This process makes network monitoring simple and effective.

Spend and save

Assuming the customer is the right 'fit' for the technology, the premium paid for IIM on day one is easily offset by the savings achieved through process improvements and greater operational efficiency. Return on investment really depends on the degree to which the system is deployed and how it is aligned to and utilised by related processes and applications. Deployed and used correctly, it is quite feasible for the initial outlay to be recouped after 12-24 months.

The vast number of benefits it brings to every level of the organisation, as well as the long-term cost savings, makes IIM a justifiable investment for many businesses. However, comprehensive end user training is key in order to receive the maximum benefit and to experience its entire range of features.

The way forward

Efficient network infrastructure management comes down to a combination of best practice and the use of the most appropriate technologies. Given the importance of uptime and the ability to identify and remedy problems quickly, the fact that adoption of IIM is growing is no surprise and as this technology becomes more refined it will provide exponential benefits to a businesses of all kinds.