



Open networking brings automation benefits

As organisations grow and evolve, the needs placed on IT infrastructure change and can prompt adjustments to broader IT strategy. These changes to IT strategy can also arise from new technologies providing significant benefits over existing systems.

Most IT managers face the regular challenge of deciding how and when to adopt new technologies, but many of these decisions are focused on the more tangible hardware and software components. So rethinking how networking can be optimised for new business needs or technology developments is often a very low priority.

A recent project to develop an IT networking plan for a research organisation highlighted the recent transformations in open networking technologies and the need to put more emphasis on this often overlooked area.

The organisation is moving to a new purpose-built research and innovation facility in Bristol, and wanted CFMS to develop an IP-based Ethernet network to support its business operations. The building comprises a mix of office spaces used by staff, collaborators and visitors, and test cells containing a range of equipment for research and testing.

The research organisation network will have to provide connectivity across the facility for users and test cell systems, and all building services, including the building management systems, access control, alarms, CCTV and other services.

When defining the system requirements, the research organisation wanted a highly reliable network, which could resist the impacts of

unforeseen hardware and software failures, with minimal impact to service or administrator input required. So a design was sought to ensure there are no single points of failure or other key infrastructure.

The research organisation also wanted systems that could be managed and maintained with a lean administration. Conventional network management requires considerable administration, and configuration is managed by an administrator applying changes manually via the command line.

This approach can now be superseded by using automated network management, which allows network administrators to define a configuration state and allow automation tools to maintain network performance.

This also enables administrators to deploy the 'infrastructure-as-code' (IaC) concept, which allows better testing and change control, reduces or eliminates human error from configuration changes and simplifies backup strategy.

Given the significant benefits conferred by this concept it's perhaps surprising that more IT managers have not adopted it. But to adopt this amount of automation is notably easier if open networking is also adopted.

As different hardware and software vendors use different tools and configurations, it can be difficult to implement automated network management. But the obstacles are easier to overcome now that more application programming interfaces (APIs) are available for a growing range of operating systems and software tools.

Open Networking disaggregates its hardware and software, hardware can be matched to the requirement, regardless of manufacturer while continuing to run a consistent network OS and interface.

The facility's network will be used by a range of services, and a mix of both staff and visitors, so network security needed careful planning. Instead of simply building an implicitly trusted network inside the corporate firewall, different devices were configured on different virtual LANs, separated with a security appliance.

Like network configuration and maintenance, security can also be automated with open networking, so security administration is also much easier. Boundaries between different VLANs can operate with automated rules-based filtering to control which users can access different areas.

As the project is a new building in a green-field location and with the principles of automation and centralised configuration management, the network plan was built to meet the facility requirements for security, redundancy and to

fit physical constraints. As there was no need to combine existing infrastructure into the plan, all aspects of the plan were conceived to offer the most appropriate performance to meet the requirements of the research organisation.

In addition to proposals for network facilities, the plan also included recommendations for operational systems and processes to make the most of the latest automation technologies. Ansible was selected to manage the configuration of Linux, Windows and other network appliances.

As well as providing core IT functions, an agile, automated network infrastructure built from digital engineering principles will also help to create a culture of innovation. The systems are not constrained like conventional IT networks, so will contribute to forming a creative and dynamic organisation.

The research organisation facility had the benefit of starting from scratch, but these approaches are equally applicable (with careful planning) for existing IT systems to adopt these methods. If you would like to adopt more open networking and automation, talk to our Engineering Computing Services team at CFMS.

CFMS
Bristol & Bath Science Park //
Dirac Crescent // Emersons Green //
Bristol // BS16 7FR
w: cfms.org.uk
e: info@cfms.org.uk
t: 0117 906 1100