



Building Security and Cost Savings into Shared Networks for Local Government – Transformational Network Models

This paper outlines the different approaches to creating shared networks for local public sector bodies and the relative benefits of each.

Introduction

In the years since the publishing of the original Transformational Government report, networks have played an increasingly important role in public sector organisations. The drive for cross service collaboration places new demands on wide area networking infrastructures, and has shifted their importance in the effective delivery of technology for government.

The focus on greater efficiencies in service delivery and more effective collaboration continues to grow. While this clearly starts at the human level, the building of shared infrastructure has an essential part to play in realising the desired cost savings.

“Modern, effective public services rely on public bodies sharing information in order to provide a better and more joined up service for our customers.” **Sir Gus O’Donnell, Cabinet Secretary.**

Operational efficiency is difficult to achieve when services are run across disparate, disconnected IT and communication networks. Efficiency comes from being able to manage your infrastructure and the overall user experience within a single environment. That opens up key questions about how far your network infrastructure extends, and who makes use of it. For example, meeting productivity and value obligations, while compromising on security, is costly in the long run. Different options must be explored and evaluated.

Security in the Context of Shared Networks

Protecting restricted data is a top priority, and a secure network infrastructure has an essential role to play in enforcing security guidelines and ensuring compliance. Confidentiality, integrity and

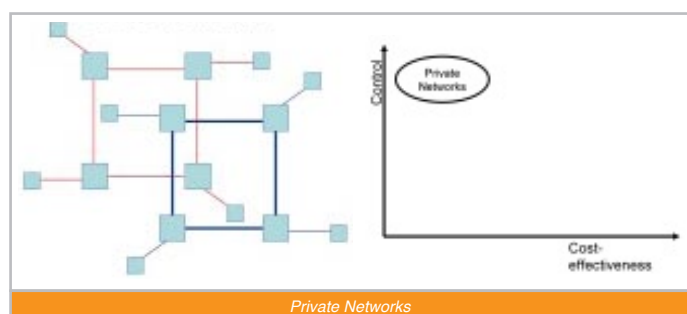
availability are at the heart of a secured network. In the past, the security requirements to maintain network integrity between different public sector organisations were agreed on a case by case basis. More recently, broader compliance with standard Codes of Connection at the local level have opened up the potential for greater interconnection of systems. Firewall layers at network boundaries protect confidentiality and availability, while network-based quality of service can ensure availability even in times of crisis demand.

Local government organisations can take advantage of this combination of frameworks and mature technologies to take new approaches to building shared networks that can still interconnect securely with central government.

Traditional Network Models

Private Networks

The traditional approach to wide area networks involved building out dedicated infrastructures. This private network model provides a high level of control, but costs are also high and the resulting infrastructure is relatively inflexible. A single owner bears the full cost of the infrastructure, and any moves and changes require physical additions or changes to the network.

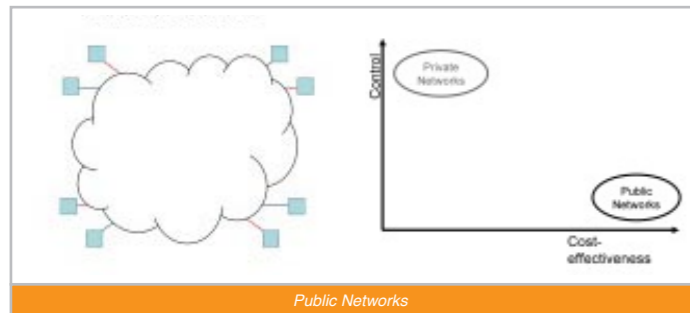


Private networks can best be described as a high-cost, high-control model. The traffic on the network can be known and profiled, and physical separation provides the base level of security. The network can be run at a high level of trust, but application level security and layered firewalls are still required to meet security criteria.

Availability also comes at a high cost, since the price of building resilience into the design cannot be shared across multiple users. The legacy of private networks is multiple, isolated infrastructures, built to different standards and with different technologies, resulting in costly, inflexible solutions.

Public Networks

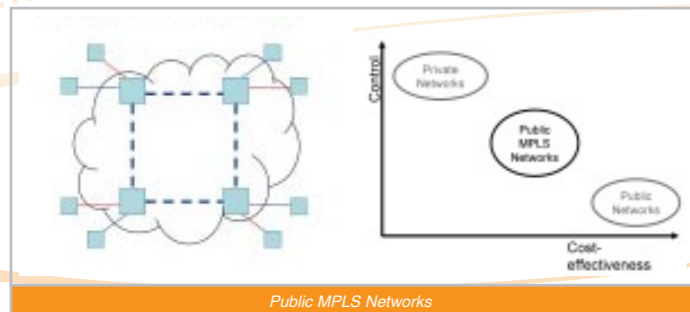
Although the public network with the longest history is the Public Switched Telephone Network (PSTN), it is the Internet that has now become the de facto public network infrastructure. As a global network with multiple owners, it is the antithesis of a Private Network. While application and network level encryption can be used to protect data from eaves-dropping and modification, the underlying infrastructure is comparatively insecure, and service level guarantees are minimal.



The Internet is best described as a low-cost low-control model. It has both the advantages and disadvantages of a one-size-fits-all solution. Users share the infrastructure on equal terms, while security is left to the application layer. This limits its reliability and leaves it open to denial of service attacks, but it does provide a new, low-cost channel for interaction with citizens, businesses and community organisations.

Public MPLS Networks

In the 90's, in parallel with the emergence of 'The Internet', network operators built out networks on shared infrastructures that used logical separation to provide "private" networks, on a public network infrastructure, often called VPNs (Virtual Private Networks).



Early versions of these networks used Frame Relay or ATM (Asynchronous Transfer Mode) technology to provide separation and control of each customer's traffic. Their modern counterparts employ MPLS (Multi Protocol Label Switching) to achieve the same effect, providing logical isolation of traffic, traffic engineering and Quality of Service to meet the requirements of a broad range of networked applications.

MPLS is highly optimised for the delivery of advanced IP-based services, and has become the modern standard for wide area networks. Public MPLS services, while providing clear cost advantages over building a dedicated private network, are still relatively expensive when compared to the Internet, but with a lower level of control than a dedicated private network.

One of the limitations of these "private" public networks is that they are constructed around standardised service descriptions. This is a necessary compromise to support a broad range of users, with widely differing demands, without becoming unmanageably complex. A network built to provide generic IP services as well as meeting industry specific demands from sectors as diverse as finance, retail, manufacturing, entertainment and government cannot always resolve the conflicting pressures on price, security, functionality and 'robustness'. Compromise is an inevitable part of service design in such environments.

Standardising service design also means that there are conflicting demands on service windows, controlled outages, and "adds, moves and changes". The equipment used in the network is not always security accredited and operational procedures are often at odds with government security requirements. This can often leave public sector organisations short changed, or can eliminate the option of using such networks altogether.

While there are clear economic advantages to re-using a single physical network across multiple customers, this presents the added challenge that in periods of extreme demand, such as a state of emergency, the network has to accommodate all of its users as well as critical public service organisations. And some network operators also run their public Internet services over the same platform, raising further questions about security and availability.

Transformational Network Models

So, is it possible to retain the security and control of a private network, while realising the cost benefits of a shared network? More importantly, can this be achieved as part of a more strategic move towards a transformed network infrastructure?

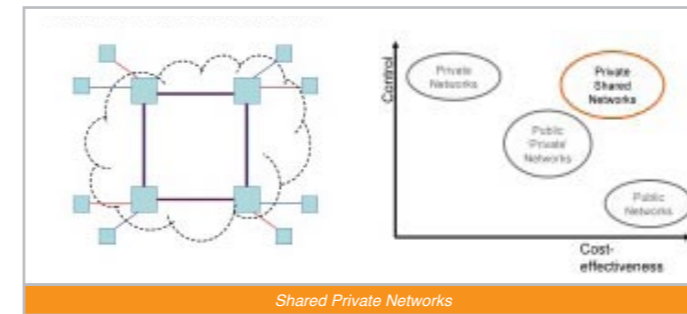
Public networks provide a cost effective way to extend digital services to the general public, but do not meet the security requirements for sensitive data and cross-body information sharing.

Public MPLS networks appear to balance privacy and cost, but are challenged by the requirements of many different types of user and lack of service features.

And given that private networks do not meet the requirements for cost efficiency, collaboration and sharing across public bodies, a different network model is required to provide a way forward for public sector organisations. A shared private network.

Shared "Private" Networks

This transformational network model delivers the best fit for public sector organisations. It delivers a competitive price point and a path towards better collaboration.



Local government bodies have sufficient scale that sharing network infrastructure between them can deliver the same economics that made public MPLS networks so compelling, but without the need to compromise the network with other users. So not only can the cost of the network be reduced, but by focussing specifically on public sector organisations the network can be tailored to user requirements and remain compliant with standard codes of connection.

In this shared private infrastructure, each organisation has the benefit of a logically separate network, running over a single secured infrastructure. Advanced MPLS features can be used to control, separate and secure the network traffic, and the network platform is not shared with other users. This enables a feature rich MPLS deployment that can make use of advanced services such as multicast support, encrypted LSPs (Label Switched Path) and flexible IP addressing. These are features that are usually unavailable on public MPLS networks, but can be enabled in a purpose-built shared network environment. They can be used to increase efficiency of data transport, for example, by broadcasting video through IP multicast, as well as building in greater control through specific traffic prioritisation schemes.

To be both efficient and effective, network resources must be prioritised between different applications on the Wide Area Network. Voice, web conferencing and email have different requirements, and resources need to be dynamically allocated during peak periods, and in the face of unusual demands, such as a state of emergency. Quality of Service can be enabled for everything from Voice over IP to bulk data transport. Because the network is built purely for public sector organisations, the service descriptions can be tailored to specific application requirements, rather than being limited to 'off-the-shelf' service descriptions.

The users of the network can agree and standardise security practices, and make use of a network infrastructure with accredited equipment. Maintenance windows can be brought in-line with operational requirements, and the network managed by specialised staff in a way that is compliant with the unique requirements of the sector.

Technical, procedural and physical design can all be arranged specifically to meet user requirements, while the network itself is built out with the best mix of radio, copper and fibre technologies, to deliver best value. Access control and continuity can be designed into the network once, and reused across multiple applications.

Removing the Barriers to Implementation

It has been said that, for local government, some of the biggest challenges lie in finding both the money and the people to deliver change. By pooling public sector network requirements to architect a purpose-built shared infrastructure, greater opportunities for collaboration open up, without compromising security.

This shared approach makes it easier to find the necessary resources, supports local relationships and makes change easier to manage. Bringing in a knowledgeable partner, experienced in industry best practice, to combine disparate legacy networks into a consolidated infrastructure, also meets with the innovation requirement to share knowledge more systematically within the government IT community, and work with other sectors.

A transformational network provides the benefit of enabling single peering points to interconnect with central government services, while still allowing cost-effective local interconnects with regional services. This is something that both individual and national network services are unable to provide. Because the network is local in nature, it opens up opportunities for extension to more remote locations, while preserving the integrity and security of the network. Services can be extended out to key partners and workers, supporting local strategic partnerships and increasing the efficiency of service delivery.

Migration from existing private networks can take place in managed phases, to align with purchasing cycles and preserve existing services, while bringing new users onboard.

Above all it's most important to work with a specialist network provider, such as MLL Telecom, who can build you a shared private network and won't just offer you their standard network service. MLL Telecom has been serving the needs of Local Government, Police Forces, Emergency Services and the NHS for many years, and understands how to solve the unique challenges facing the public sector.

MLL Telecom Ltd
Medina House
Fieldhouse Lane
Marlow
Buckinghamshire
SL7 1TB

Tel: +44(0)870 241 7315
Fax: +44(0)870 241 7316
Email: enquiries@mlitelecom.com

www.mlitelecom.com