Evaluating networking technologies

Navigating through the latest range of networking solutions can be challenging for enterprises aiming to improve their productivity and efficiency. They need to select the combination of networking technologies that best fit their current environment and their organisation's future needs.

yes

OPTUS

Executive summary

This paper is designed to provide an introduction to the main networking alternatives available today that can improve communication across the different parts of an organisation. Whether it is an older network or an assortment of legacy and IP infrastructure, the goal of this paper is to enable an organisation to make critical long-term networking investment decisions with greater confidence.

Its main focus is the latest developments in Virtual Private Network (VPN) technology. These allow enterprises to build private data connections between their offices and other sites using virtual services rather than dedicated physical infrastructure, which can be more expensive and inefficient to run.

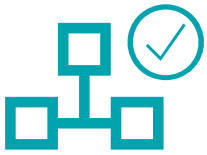
Two recent developments in VPN technology have occurred in the switching and routing layers of the network – Layer 2 and Layer 3, respectively. They were designed to help organisations by delivering improved efficiency, productivity and scalability across their Wide Area Networks (WANs).

- In the Layer 2 environment, the latest technology is known as Virtual Private LAN Service (VPLS).
- In Layer 3, it is called Multi Protocol Label Switching (MPLS).

Both technologies are capable of generating substantial efficiencies for enterprises, but there are important differences that need to be weighed up.

For instance, VPLS delivers a Layer 2 network that allows organisations to deliver any networking protocol to their sites. However, with this type of network, there is a higher management overhead for the enterprise, as the carrier does not manage the network routing, which is the enterprise's responsibility. Layer 3 solutions can be managed (fully or partly) by a telecommunications carrier or service provider and offer flexibility in the integration of other services, such as mobility, satellite and remote access solutions. Meanwhile, some organisations are best served by a hybrid solution using a combination of both Layer 2 and Layer 3 networks.

This paper considers these and other strategic, technical and financial questions that will help simplify the decision as to which technology, or combination of technologies, is best for each organisation.



Networks have changed

Traditional dedicated leased line networks based on point-to-point copper, fibre or radio connections are business grade and highly secure. However, compared to the latest network technologies, they are relatively costly to install and maintain, and the network topology on which they are based is relatively inefficient.

For example, the only site with a dedicated link to all the others is generally the head office, and this means all other inter-site traffic has to be routed through it, even if communication is solely between two branch sites. The high cost of running this sort of network is ultimately borne by the enterprise in the form of high upfront and recurring charges.

Origin of VPNs

The alternative, establishing a dedicated leased line between every branch site, is not cost effective. Point-to-point dedicated networks are also relatively difficult, not to mention expensive, to scale, and do not make the most efficient use of scarce network resources such as bandwidth. For example, the connection between any two sites is idle unless information is actually being transmitted across the link, wasting bandwidth that would be better used to improve performance elsewhere in the network.

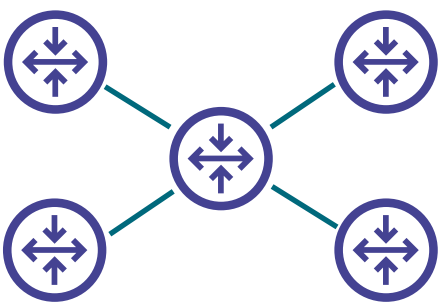
Many organisations also have challenges in managing the traffic themselves, as a dedicated leased-line network has no ability to provide awareness of the applications running over it. This means they are unable, for example, to dynamically prioritise traffic in line with the organisation's specific uses as needs change during the business day.

Virtual Private Networks, or VPNs, overcome many of these limitations by creating secure connections between sites using shared rather than dedicated infrastructure. The later use of packet-switched IP rather than circuit-based infrastructure has made VPNs even more efficient, by allowing organisations to exploit the total available physical capacity of their networks.

Although VPN infrastructure is shared by many organisations, they are each given a dedicated segment of a transmission signal for their own data stream, which amounts to a more efficient use of bandwidth and a much cheaper option than dedicated private leased lines.

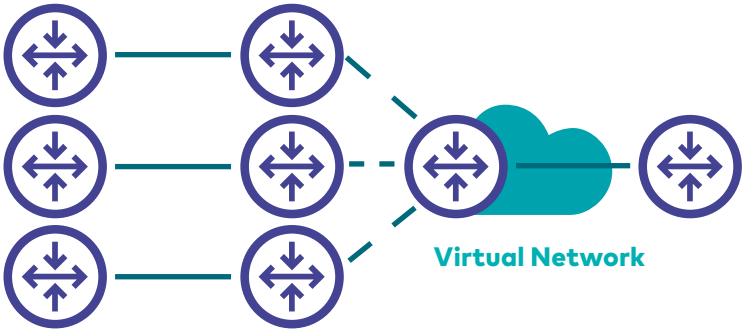
Point-to-point (private) network

Are also known as lines, private leased lines, private circuits, data lines etc.

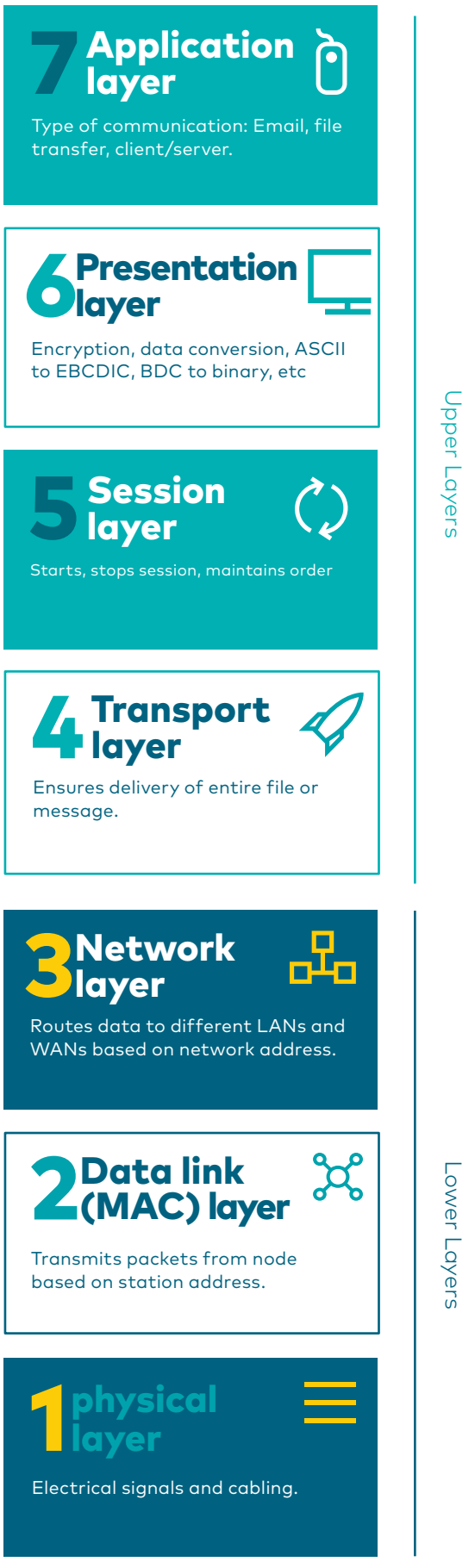


Virtual Private Network

All sites connected on a shared infrasturcture.



OSI model



Next-generation VPNs

Newer developments in VPN networking technology offer further benefits to organisations and their end users, with the main advances being in Layer 2 and Layer 3. Under the Open Systems Interconnection (OSI) model, Layer 2 is the switching layer and Layer 3 is the routing layer of a network. The latest technology in the Layer 2 environment is called Virtual Private LAN Service (VPLS). In Layer 3, it is Multi Protocol Label Switching (MPLS).

These two technologies have been designed to bring improved networking efficiency, functionality, scalability and Quality of Service (QoS) to VPNs. Their availability means enterprises have the opportunity to align their communications networks with their dynamic business or organisational needs more closely than ever before. The implementation of QoS and MPLS/ VPLS means that the network's performance can be dynamically altered to support the needs of the business.

If an organisation is seeking a state-of-the-art business-grade VPN to link its various sites, the choice is really between VPLS and MPLS, although a hybrid solution that combines the best features of each technology might also be considered.

Today's choices

There are several approaches to creating Virtual Private Networks in Layers 2 and 3 of an enterprise network in addition to VPLS and MPLS. These range from Permanent Virtual Circuits (PVCs) based on Frame Relay and ATM protocols to Ethernet-based virtual LANs (VLANs), Dial VPNs, and IPSec tunnelling over the Internet.

Layer 3 VPNS

In a Layer 3 VPN, sharing takes place at the routing layer using IP technology. Solutions include Internet-based IP VPNs, private carrier IP networks and, most recently, IP MPLS.
Layer 3 VPNs have the advantage of flexible, any-to-any connectivity. Every site in a Layer 3 network, for instance, is able to connect directly to every other site.

Another advantage of IP-based solutions in general is that they allow content to be separated from the underlying network, which means you don't need to deploy additional specialist technologies in order to dynamically manage different traffic types such as voice, data and video content.

1. Internet-based VPNs

An Internet-based VPN is one that establishes a private network using the infrastructure of the public Internet. While these services tend to be cost-effective, they are not business-grade in the crucial sense that there is no adequate guarantee of packet delivery, speed, QoS or security.

The only guarantee given to the organisation is 'best effort' routing of its packets. Moreover, to maintain overall network performance and packet security, it is necessary for the organisation to deploy a network gateway device that is able to encrypt and decrypt data very quickly. This gateway must also be able to process several tunnels simultaneously.

To make such a network secure enough requires considerable engineering resources to ensure a suitable level of encryption, as well as the presence of on-site security engineers to make certain the environment remains safe. However, Internet-based VPNs can be useful in allowing cost effective remote access through shared devices, either managed by the Enterprise or the Carrier.

2. Private IP VPNs using MPLS

MPLS is the latest-generation in IP VPN technology. It was developed to address the fact that an IP network prior to the implementation of MPLS was unable to offer the quality of service necessary for real-time services like voice communications and video conferencing. MPLS delivers QoS by forcing traffic between network nodes to follow a particular path through the network using Label Switched Paths (LSPs). LSPs direct various types of traffic along certain designated paths, while non-labelled traffic is routed on a 'best effort' basis. The switching aspect allows the traffic to travel much faster than if it was simply being routed through the network.

MPLS also enables application-specific traffic engineering, which means a network manager can design different paths for different types of traffic. For efficiency, the most demanding traffic could be allocated the shortest route, or to different routers to minimise the likelihood of congestion. While MPLS can force packets along specific paths, it cannot by itself provide QoS. For that, a traffic engineering technology known as Differentiated Services Code Point (DSCP) is used. This allows IP packets to be differentiated according to the organisation's QoS requirements.

Layer 2 VPNS

1. Virtual Circuits (VCs) and Virtual Paths (VPs)

In a Layer 2 VPN, the network is shared at the switching layer. In addition to VPLS, Layer 2 solutions include ATM, Frame Relay, Ethernet and Metro Ethernet. A number of these solutions are based on highly secure Virtual Circuits (VCs) that enable the carrier to assign dedicated bandwidth to each organisation, as well as offering service level guarantees.

Typically, a carrier charges separately for each PVC that an organisation deploys. ATM solutions additionally make use of Virtual Paths (VPs), which are classes of virtual circuits created to allow different traffic types, for instance, voice, data and video, to be segregated, in order to travel around the network more efficiently.

2. Ethernet Services

More recently, carriers are offering Ethernet VPN services using Virtual LAN (VLAN) technology. This works by deploying Ethernet, traditionally a LAN technology due to its distance limitations, at Layer 2 to enable it to span over larger areas. These distance limitations have been overcome by the development of switched Ethernet, which has enabled it to become effectively a WAN technology.

At the same time, new optical-fibre standards have paved the way for high-speed Ethernet communication over metropolitan distances. Layer 2 Ethernet WAN services use the Media Access Control (MAC) addressing scheme for sending and retrieving data.

The Ethernet switch associates a particular MAC address (or group of addresses) with a specific port and switches the traffic accordingly. As with virtual path solutions, traffic can be segregated for greater efficiency.

3. VPLS

Despite it being possible to build long-distance switched Ethernet networks, as discussed above, native Ethernet does not scale very well and Virtual Private LAN Service (VPLS) was created to overcome this problem. VPLS networking works by extending the LAN from each organisation site to link up with a single bridged LAN created by the carrier.

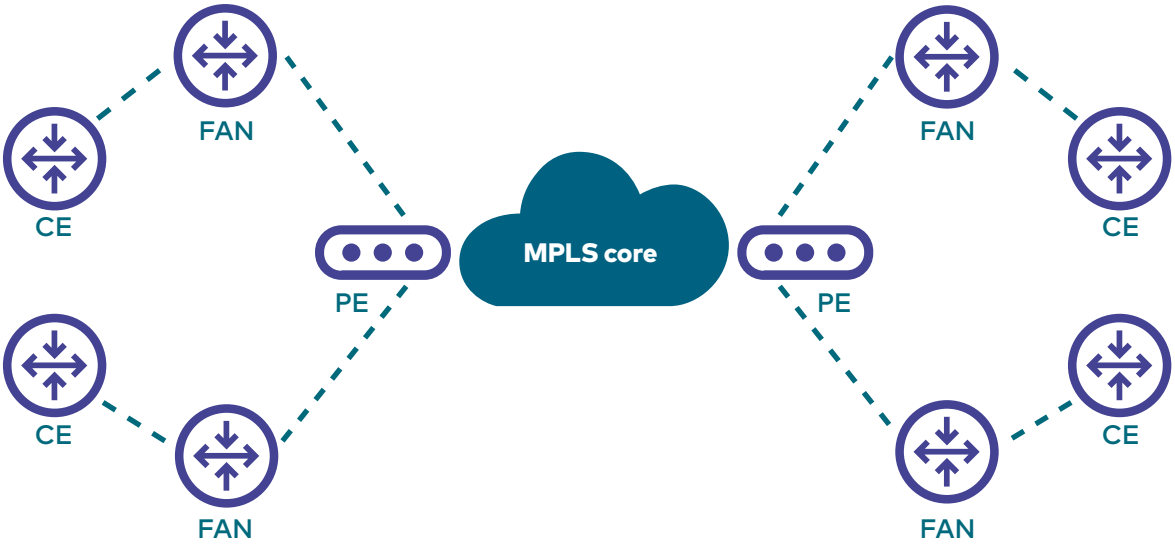
While MAC addresses are used to switch traffic between sites, labels (an MPLS network) are used to switch it across the core. This multipoint setup is simpler to manage than earlier Ethernet solutions, and as well as removing limits on the spanning tree network size, it offers more consistent traffic engineering capabilities.

With VPLS, when a new location is added to the VPN, connectivity is automatically established between the new location and every existing location without having to change the networking and routing for the existing locations. This can be a significant benefit to organisations that are changing their corporate locations regularly.

MPLS and VPLS were designed to help organisations by delivering improved efficiency, productivity and scalability across their Wide Area Networks (WANs).

Optus Evolve

Ethernet 802.1Q	Provider Bridge IEEE 802.1ad Q-in-Q	National Connectivity Ethernet + MPLS	Provider Bridge IEEE 802.1ad Q-in-Q	Ethernet 802.1Q



FAN = Fibre Access Node CE = Customer Edge PE = Provider Edge

Making your decision

Choosing which type of network to use is an important decision. This section is designed to help the evaluation process along by outlining the key strategic, technical and financial factors that need to be considered.

Are QoS and bandwidth service level agreements required?

If an organisation is looking for the lowest possible cost, then a solution using the public Internet is possible. However, such a solution is not business-grade in that there is no guarantee of packet delivery, speed, QoS or security.

When it comes to selecting the appropriate technology for an enterprise, it is important to keep the overall business goals firmly in mind. Is network consolidation the ultimate objective? Is the aim to reduce costs or administrative overheads by unifying multiple networks in the most efficient way? Consolidation certainly makes sense because operating numerous Internet gateways tends to multiply service costs, as well as creating administrative and security headaches.

Are there a large number of corporate locations?

If more than 20 corporate locations need to be connected, a Layer 3 solution (or a hybrid solution) will be required because carriers typically restrict Layer 2 services to 20 sites due to addressing limitations.

Another important factor is that a Layer 2 solution will require dedicated resources to be available at each site to manage the network, which may not be feasible if there are a large number of locations.

Are there technical resources on-site?

With a Layer 2 network, the enterprise effectively purchases a series of large pipes that connect its various sites together. The carrier's role typically ends there, and thereafter the organisation is responsible for managing its traffic over the network, as with a traditional local area network (LAN). To reflect this difference, Layer 2 network capacity is typically cheaper for the organisation to purchase.

Layer 2 VPLS has the advantage of being a conceptually straightforward solution supporting all network protocols. It also allows organisations to control Layer 3 routing and addressing, and works with any Customer Premise Equipment (CPE) that has a bridging capability, while MPLS has the advantage that the carrier absorbs all of the Layer 3 complexity and that no special CPE configuration is required for any attachment type.

Who will manage the network?

A crucial consideration is the extent to which the enterprise wants to, or can, manage its own virtual private network. IP-based Layer 3 VPNs are application-aware, which means once installed the organisation doesn't need to manage address schemas or traffic, which simply routes to the relevant IP address. The carrier, in other words, takes care of network management and makes sure traffic gets where it needs to go, when it needs to get there.

With a Layer 2 solution such as VPLS, however, the carrier has no visibility of the packets, so an organisation needs to manage its own routing. A Layer 2 solution is thus suitable for an enterprise that has sufficient resources and technical engineers on site to manage the necessary routing configuration. Highly skilled personnel within the organisation will be needed to ensure everything is set-up correctly, that the LANs are protected and that occurrences like broadcast storms are properly averted.

The level of control required could be a determining factor. A Layer 2 network leaves an organisation totally in control of the networking and routing decisions and is typically preferred by organisations that want to keep this level of knowledge entirely within their enterprise to ensure maximum security of their underlying packets. This may be important if an organisation is operating in a heavily regulated environment where documented processes and accountability are essential.

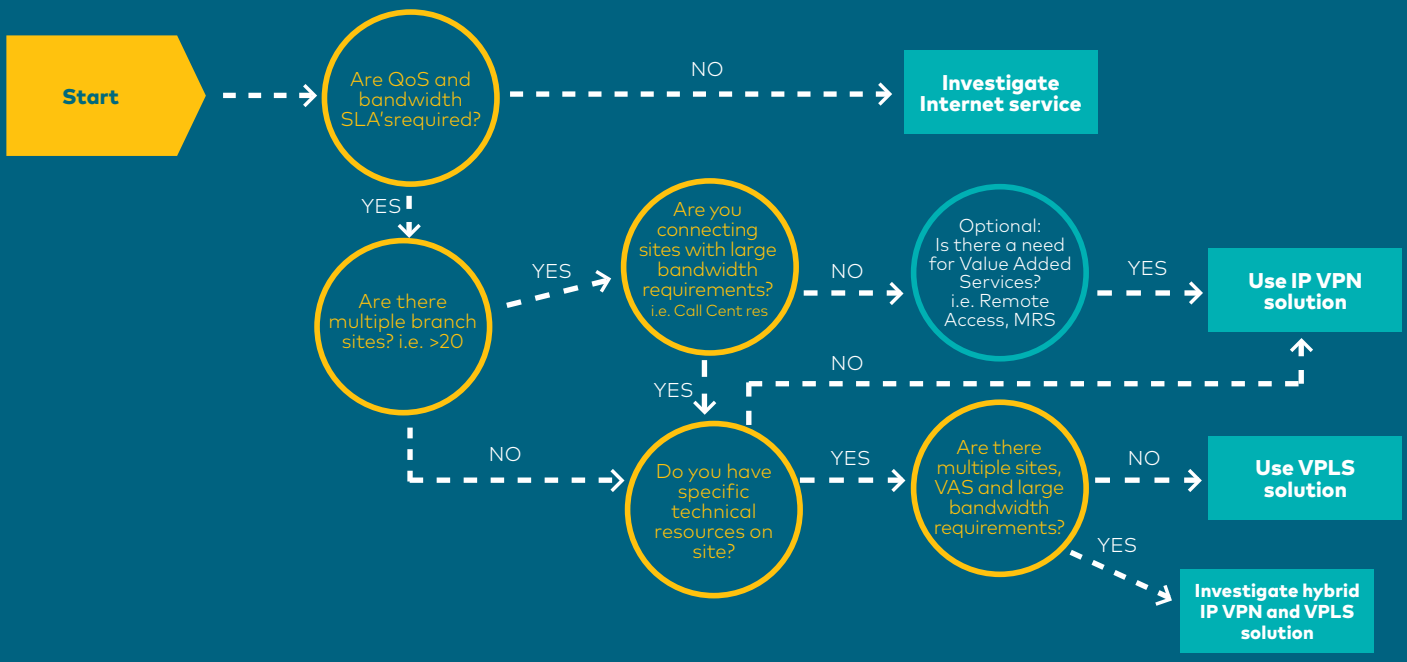
On the other hand, some organisations would prefer to have their IT resources assigned to core business and want to outsource the networking and routing decisions to a service provider. In this case a Layer 3 network is the better option. With a Layer 3 solution it is possible to outsource even further with additional value added services such as managed router and remote access services.

How secure will the network be?

Security is almost identical between Layer 2 and Layer 3 solutions. This is because both use secure Label Switched Path (LSP) infrastructure to deliver traffic, where inherent isolation of the inner MPLS label offers protection from Distributed Denial Of Service (DDOS) attacks from any neighbouring VPN. The carrier can also hide addresses in the core network to protect shared resources from intrusion. The only discernible difference is that an organisation using a Layer 2 network is potentially vulnerable to an internal switch-related attack.

It is important to keep the overall business goals firmly in mind

Choosing a network



Are there legacy requirements?

If there are legacy applications requiring protocols such as SNA, DECnet and others, a Layer 2 service will be required as Layer 3 only supports IP-based applications. Most enterprises today are moving away from legacy application protocols to IP-based applications, and it may be worthwhile to consider doing this rather than catering for the legacy protocols into the future. If a Layer 2 implementation is being considered, consideration should be given as to whether it also needs to support an existing ATM or Frame Relay infrastructure. If so, the consolidated network needs to incorporate those technologies. If not, the enterprise needs to consider what level of quality of service is required. If QoS support is not required, the organisation can select whichever of the available Layer 2 services – ATM, Frame Relay, Metropolitan Ethernet or VPLS– best suits its bandwidth, geographical and cost requirements.

Is there a mobile workforce?

If a mobile workforce or if remote commuting is part of the organisation's disaster recovery plan, then ease of remote access may influence the decision. With a Layer 3 network, a carrier may provide a value added service that enables secure remote access to the corporate IP VPN through the Internet. This enables a mobile workforce, as well as partners and suppliers, to gain access to corporate resources from any Internet-connected location. On the other hand, a Layer 2 network requires an organisation to implement and manage their own remote access solution.

What about a hybrid solution?

It is worth bearing in mind that hybrid VPLS/MPLS solutions are also possible, and even advisable in some cases. For instance, an enterprise might find it most efficient and effective to run VPLS for communication between its major branch sites and MPLS to small branch locations.

Evaluation summary

The table below provides a useful summary of the relative benefits of VPLS and MPLS compared to legacy Layer 2 implementations such as ATM or Frame Relay.

Customer requirement	Layer 2 legacy	Layer 2 VPLS	Layer 3 MPLS
Cost Reduction			
Convergence		User Managed	Remote and Mobile
Open Savings			
Ease of Management			
Integration		LAN Extension	
Visibility and Reporting			Application Aware
Connectivity			
Access Agnostic		Symmetric Only	
Between Offices			
Remote Access			
Corporate Mobility			
Remote Working			
Hot-desks (WAN based DR)		User Managed	Remote and Mobile
Scalable Network			
Flexible / Responsive			
Able to be Customised			
Security			
Data Integrity			
Disaster Recovery			
Business Applications			
Application Enabler			
Customer Communication			
Information Sharing / Accessibility			
Customer Intimacy			

Poor Good

Making the most of your network

Innovations in networking technology have provided organisations with an unprecedented opportunity to make their communications infrastructure more efficient, flexible and secure. At the forefront of this innovation are technologies such as IP VPN, VLAN, VPLS and MPLS, which dramatically improve performance by leveraging shared rather than dedicated infrastructure.

To make the most of this opportunity, organisations need to understand what each new technology does. Following that, they need to consider which of the available technologies, or which combination, is best suited to the specific applications that the business needs to support.

Give us a call

To discuss how Optus can help you through innovative communications solutions, **contact your Optus Account Manager or call the Optus Business hotline on 1800 555 937**

Join the conversation

1800 555 937 optus.com.au/business

@optusbusiness yesopt.us/blog bit.ly/OBLinkedIn

OPTUS

GMO_N 0385 0816MZ