



# Retail IT Buyers Guide

Investigation: Retail Networks – Best Practices

Simon Brassington

# Retail WAN Networks...

## ...IT Buyers Guide

### Foreword

The following guide was created to help individuals like you, with the responsibility for managing your IT infrastructure, to help you with one or more of the following:

- Provide a better understanding of what private networking is and **why it's the best network choice for Retail organisations.**
- Help better understand upcoming technology's like SDWAN.
- Help you select a Service Provider who can meet your exact business needs and **provide service excellence.**

I was Head of IT for a major retail organisation for many years before designing retail focused networks and services at Blaze Networks. I understand the challenges you face on a day-to-day basis as well as the pressures on budgets.

I've also provided some detail on the network we built for retail organisations like yours, so you have a benchmark to compare suppliers to.

I trust this guide will prove useful and make your life easier. Please feel free to contact me if you have any questions about private networking or specifically about our purpose-built Retail Private Network or, in fact if you'd like more details on any of our retail IT solutions that make up our retail defined IT services portfolio.

My personal contact number is **01625 506778**



Warmest regards,

A handwritten signature in black ink that reads "S. Brassington". The signature is fluid and cursive, with a long horizontal stroke at the end.

Simon Brassington  
Technical Director and Retail Specialist

# Contents

Why Retail Organisations are Moving Towards Private Networks..... 3

Must Ask Questions of an MPLS Service Provider.....8

Blaze Networks Testimonials..... 19

10 Reasons to Choose our Retail MPLS Network ..... 21

# Why are Retail Organisations Moving Towards Private Networks?

As your motivation for reading this guide is to help you make an informed decision about subscribing to an MPLS service, it can't hurt if you know a bit more about the different service options that are available to you.

My intention is to help you understand why Private Networks are a better alternative to more traditional WAN services, especially IP VPN services and some of the security and compliance challenges these create.

The main reasons **retail organisations are migrating to private networks** are usually:

- More bandwidth for less money to address budget constraints
- Guaranteed levels of service (QoS) to enable the deployment of network performance related applications like voice, video and the more recent in-store customer experience applications buyers demand.
- Increased availability and redundancy to ensure store transactions are never affected
- Flexibility to:
  - Allow the creation of temporary "Pop Up Stores"
  - Address the necessity to close stores or move location
- To assist in achieving PCI DSS compliance and the new legislation General Data Protection Regulation (GDPR).
- To have a specialist company look after the communications for the Business.
- To have SDWAN services and benefits can be made available.

## Questions to Ask Yourself:

***One of the first questions to ask yourself is how much do you want to outsource?***

If you're a retailer with two overworked networking staff, outsourcing everything is very attractive. If you're a larger organisation with in-house expertise, then you may not want to pay for a service you can do yourself, but...

You do have to ask yourself if this is the best utilisation of the resources you have, when a Service Provider can take advantage of the economies of scale and do it for you at a much better price point; especially when competent CCIE engineering resources can be an expensive asset.

### ***A second question is whether cheaper IP VPN services are adequate?***

There are a number of factors to consider, which I'll explain in a minute, but more often it comes down to the size of your business and how many stores you have.

Once you go over about 10 stores, then the cost, the management, the security considerations and the ability to stay on the right side of compliance would lean towards a private MPLS service from a PCI-DSS certified Service Provider.

Note that when we say reputable, we don't mean large (expensive) Tier 1 Service Providers like BT. Smaller businesses offer the same technology but are usually more flexible in what they can do for you, they typically cost less and offer greater, more personalised levels of service.

### ***A third question to consider is: do you require a single Service Provider or dual Service Providers for redundancy?***

With a sole Service Provider solution there's always the risk of "lock in", especially if you are signing long term contracts to try and get a better rate.

The key benefit of a dual Service Provider solution is, as we've said, about being able to take advantage of having redundant links and therefore higher availability and be less susceptible to outages.

It's often said that having dual providers also gives you some bargaining power to enable you to drive down prices and get the best deal.

With all that said, your management overhead and associated cost will increase.

The "finger pointing" between Service Providers when you do have an issue, can seriously delay fault resolution and directly impact business performance; and **no IT Manager wants to be held responsible for that.**

When I was Head of IT for a major high street retailer, I always looked at finding an independent company that could provide a dual Service Provider solution and manage everything for me. They can negotiate hard, using their economies of scale to get you the best price. You have one "Throat to Choke" in the event of an issue, and you can let them deal with the challenges of honouring the SLA for you.

However, with dual Service Providers, your costs may be higher, but at least your network may stay up even when one provider is having problems. By working with two Service Providers, you can pressure them on pricing, and you can also compare the levels of service they actually provide. (Experience says that sales folks make all SLA's sound great, but what you really get can be somewhat different!).

There are a number of direct benefits for Retail businesses using a private MPLS network versus a traditional VPN (Virtual Private Network) technology.

The first issue with typical VPN solutions, is they are deployed on the public Internet. Each branch location becomes an entry point from the public Internet connecting into

your secure retail infrastructure and then back to the head office. Communication is completed in most cases over a secure Virtual Private Network “Tunnel”, but let me emphasise the fact that this tunnel runs over the public Internet.

The more branches you have, the more entry points you have from the public Internet, so the more branches in your network, the bigger the problem becomes.

## Increased Network Running Costs

The first issue comes in the form of increased network running costs. There are a number of areas that need to be considered when looking at the Total Cost of Ownership of your retail estate, and the network running costs that make up part of this.

The following provides samples of some of the running cost components, costs that could be eliminated with a private network infrastructure:

- Quarterly PCI-DSS penetration testing needs to be carried out on any device connected to the public Internet.
- The equipment used to connect the branch locations to the public Internet is in most cases an unnecessarily expensive firewall, routing and security piece of equipment, but needed in a VPN deployment to keep the branch secure from the public Internet.
- The head office device that connects to all of the branch locations usually requires a very high end and, again unnecessarily expensive router/firewall that costs thousands of pounds. In addition to the purchase cost, you need to maintain subscription requirements and ongoing administration.
- Most retailers use their head office to make IT services available to the branch locations. To support this capability, a traditional VPN solution, using expensive fibre services are usually required at the retailer’s head office.

An MPLS solution uses centralised Data Centre bandwidth and is therefore considerably more cost effective. One firewall is used in the central Data Centre to provide connectivity for the entire retail estate, reducing cost and complexity.

## Increased Administration Overhead

The next issue to consider comes in the form of network administration and the increased workload and therefore increased costs that come with administering a VPN network.

Network administration costs can be significantly higher with a VPN network deployment. They are higher because there are more firewall policies to manage, more equipment and more software subscription deployments to maintain and monitor.

Change control needs to be implemented on every device in the infrastructure due to PCI-DSS requirements and can become a major headache for IT Managers with growing and evolving network requirements.

## Increased Risk

All companies today have to be aware of the risk to their business, their brand and their ability to trade when using public Internet services.

The more entry points into the Internet, and the more devices that need managing, increases the chance of human error, software defects or vulnerability that will potentially create a security breach and allow access to the retail network.

### **Reducing risk has 2 key benefits...**

1. One is by reducing costs in the form of either actual costs or through the reduction of administration overheads.
2. The other is achieved by the mitigation of lost revenues, non-compliance fines or brand damage.

Firstly let's look at how a **MPLS network saves money over a VPN solution**:

- Quarterly PCI-DSS penetration testing across all branches is not required, as no branch location is connected to the public Internet. There are only one or two entry points from the public Internet into the MPLS network. This penetration testing cost reduces by ££££ thousands for retailers with over 30 branches.
- The equipment used at the branch locations only needs to be low cost routing equipment, rather than sophisticated, highly featured CPE. This is because the branches are no longer connected to the public Internet.
- The head office no longer needs high end expensive firewalling equipment as this is outsourced to the Service Provider and implemented on the perimeter of the MPLS network, thus safely connecting the entire estate to the public Internet.

- With an MPLS network, the retailer can take advantage of low cost centralised Data Centre bandwidth and hosting. This allows the retailer to considerably reduce the amount of bandwidth required for the head office, whilst offering more resilience to the branch estate.

**Now let's address these administration and risk issues:**

With a private retail MPLS network, like the service provided by Blaze Networks, there is only one centralised firewall. This means all firewall policies and intrusion detection and prevention services can be managed on this one firewall in a high availability mode (2 firewalls stacked but managed through one console).

In addition to this, a MPLS service like ours is fully managed, so the retailer only need contact our support team for any Adds, Moves or Changes that are required.

This allows the retailer to concentrate their security investment into the one firewall entry point, again **reducing cost and increasing security** for the branch and head office estate.

In summary, any retailer investing in a private retail MPLS network will reduce risk and administration by centralising security investment and reducing the number of entry points on the public Internet.

## Must ask Questions of an MPLS Service Provider

The following provides a list of Frequently Asked and Should Ask questions, designed to ensure that the network you subscribe to, provides all the features and functionality you need to efficiently and securely run a network that meets a retail organisation's business needs.



The follow questions come from the personal insight gained when I was Head of IT for a retail organisation. They are also based on feedback from many of our personal customers with regard to what they say they need from an MPLS network.

We've also researched all the RFIs and ITT documents that we've received over the years and pulled out all the common (and some less so common) questions that have been asked by potential customers.

We've listed questions that cover 3 main areas:

- The Network
- Support
- Service Level Agreements

NOTE: We've also provided answers to help you understand what kind of response you should be looking to get.

### **Q 1. *Store availability is key, how do you provide resilience at each branch location?***

A 1. The most cost effective option is to deploy VDSL technology. To achieve N+ 1 you are best using 2 separate Tier 1 Service Providers. This configuration offers both failover capability in the branch and means that separate LLU equipment is utilised in the local exchange, further reducing any single point of failure.

Using 3G, 4G or 5G backup is another effective alternative, providing the CPE (Customer Premise Equipment) supports this feature. It is often cheaper however, to deploy a second VDSL line with a separate Tier 1 provider rather than using a mobile service. Also, the dual line solution has better availability throughout the UK due to mobile network availability and materials used in retail buildings thought the UK that impact Mobile signal.

You should also consider planning for the worst-case scenario, where connectivity is down for a prolonged period of time due to Service Provider network problems, and where your branch has only one connection.

In this situation, Blaze Networks will ship a 4G or 5G router to the location on a next business day delivery. There is no extra charge for this service. If you have purchased our retail MPLS network offering you gain access to next business day delivery of 4G or 5G equipment and our engineers will proactively contact the store to restore connectivity and allow trading as normal.

Blaze Networks have numerous options for on premises equipment that support both fixed line broadband and 4G or 5G backup through a single piece of routing equipment.

We proactively work with you to design the most cost effective and business critical solution to maximise the potential for 100% uptime across your estate.

**Q 2. *Can you offer 99.99% uptime and how do you achieve this?***

A 2. There are 2 considerations here, the core network and the branch access. As explained, there are a number of ways of ensuring failover capability and increased uptime in the network access points through the deployment of N+1 redundancy capabilities.

The same is applicable in the core of the network. You should be looking for a network provider who uses the same high availability N+1 configuration principles in the core of their network.

**Q 3. *Can't I use the much cheaper alternative of VPN?***

A 3. Retailers should not consider VPN technologies to link their retail branch locations to their head office firewall. VPN solutions are directly connected to the public Internet and as such, offer a point of entry into the network at every store. Regardless of configuration, a VPN device that is made available on the public Internet is deemed as an entry point by the PCI-DSS Security Council and therefore increases the risk of security breaches.

Our MPLS network offers the retailer only one entry point into the entire network. This one point is typically the network's core Data Centre firewall. This firewall will have greater investment in security technology, making your network more secure and less vulnerable to security breaches.

**Q 4. *Doesn't the cheap nature and therefore cost savings of a VPN solution outweigh the risk of security threats?***

A 4. NO. Although a VPN network is usually cheaper than an MPLS network (but **not always the case with our Retail MPLS Network**), there are other cost considerations that will make this network technology more expensive.

PCI DSS compliance dictates that each network entry point is “Pen. Tested” (Penetration Tested) each year to assess the posture of your network and its potential vulnerability to attack. Many retailers now have reduced obligations due to PCI-DSS certified end to end solutions. For those retailers, you still need a good security compliance standard to follow or your infrastructure will likely be very unsecure, most if not all compliance standards state the requirement for yearly Penetration testing. This is best practice and the only way a company will know if they are exposed to issues on the network. Most if not all hackers start with such vulnerability scanning followed by a deeper penetration tests so they can find out what open vulnerabilities they can exploit.

If you multiply the number of stores you have by the current Pen. Test fee (£1000/ year at time of writing this document), and times this by the number of branches for the whole year, it's highly probable that these additional costs will far exceed the cost of a more secure Private Network deployment. This is not including the security vulnerability scanning that also needs to be undertaken each quarter on both the internal and external network. In this example we are talking about PCI-DSS as a compliance standard, but this could be Cyber Essential Plus or ISO 27001, all are good security standards that should be followed by any organisation.

This doesn't consider brand damage and other less tangible factors, which only you can put a value on to your business.

#### **Q 5. *What CPE considerations should I take into account?***

- A 5. There's a few considerations to undertake when making a CPE decision and these are to do with price, compliance, throughput, features and functionality. You also need to consider the manufacturer's end to end security fabric and how your decision will impact on SDWAN offerings.

Many service providers will try and sell you low cost CPE solutions from the likes of Netgear and Zyxel, when these types of manufacturers can't always meet all your requirements both now and in the future. Cisco make exceptionally good equipment and can offer features that can cover all eventualities future proofing your investment. With leading manufacturers like Cisco, Fortinet and Juniper, you should ensure the CPE you choose integrates with their full security fabric as an SDWAN running on a private network will lower administration whilst giving a single pane of glass to manage and monitor the entire infrastructure.

WLAN capability is a key consideration today when choosing your branch CPE. Mobility “Services” are becoming very popular with retail organisations.

The ability to get secure visibility of your customer's mobile devices, and be able to push offers and point of sale incentives, in real time, to your store visitors can:

- Increase the customer experience to create differentiation
- Improve customer satisfaction and retention
- Grow sales order value

These types of services may therefore demand a more sophisticated appliance and should be considered when making your investment decisions to help protect your investment. In most cases the wireless network joins a manufacturers security fabric, so consistency with one manufacturer is key.

**Q 6. Do I need Proactive Monitoring or simply report faults as they occur?**

A 6. To maximise network uptime and fast fault resolution, you should be looking for a service provider who is actively monitoring your network for you. You are paying for a service, you shouldn't have to do this yourself.

**There are 2 main benefits from proactive monitoring:**

The obvious one is the fact that you get a much faster fault response and resolution time, but...

...you don't waste your time reporting false positives.

A good monitoring platform will give a high level overview of all connectivity and routing equipment across your retail estate in real time. If there are any issues, a real time traffic monitor will change its state and alert engineers.

Often when broadband connectivity goes down, it is only a short "Bounce" of the connection and then connectivity is restored. You should be looking for a company that will monitor the connection, looking for prolonged issues or recurring issues and act accordingly.

This can save you time and ensure network availability is maximised.

*"Blaze Networks' Retail MPLS Network has provided us with a very resilient branch infrastructure, enabling us to provide a great service to our customers. They proactively contact stores and fix any issue before it becomes business impacting.*

*Excellent company to work with, who truly understand our industry and business requirements."*

**Chris Marchant**

Company Secretary, Collectables Retail

At Blaze Networks, our engineers proactively call your store in the event of a properly identified issue and troubleshoot the connection, eliminating the need for your staff to do fault reporting!

Our Networks Operations Centre has direct access to the Openreach WLR3 engineering platform allowing our engineers to do line and broadband tests whilst on the phone with your retail location.

In addition to the engineer contacting the store, email alerts are sent to appointed people in your retail organisation so you are aware of an issue at any given location in real time.

Our customers have full access to our monitoring platform for full network visibility, ticket updates and to run appropriate reports. You can run historical or real time reports on equipment and bandwidth utilisation and much more.

This means you can ensure that Service Level Agreements and Key Performance Indicators are achieved by Blaze Networks.

We believe in complete visibility of your retail MPLS network investments and through proactive support and monitoring we reduce internal IT administration and increase your uptime across your retail estate.

**Q 7. *What Out of Hours engineering support do you offer?***

A 7. You should be looking for a Service Provider who offers 24/7 support and accept nothing less. This should not just be a response service, but a service that provides the proactive network monitoring as previously described.

***Why is this important?***

It's important because an out-of-hours fault can often be resolved before store opening time, thus **not affecting trading and revenue generating activities.**

The last thing you want is to discover you have a network failure at 0900 on a Saturday morning, when the fault happened at 10pm the night before.

At Blaze Networks, our retail customers can contact our technical support line 24/7 including bank holidays.

In addition to this, our out-of-hours engineers are proactively notified of any major network failure by our monitoring platform, meaning our proactive support approach is maintained around the clock.

Even if a store is not contactable, our engineers run copper line tests and broadband checks progressing the fault as far as possible in any out-of-hours period, to ensure the fastest possible resolution can be achieved.

Our engineers go above and beyond to ensure your retail estate is operational 24/7.

**Q 8. *What level of competence does your engineering staff have?***

A. 8 Not only should a Service Provider's engineering staff have all the appropriate industry recognized qualifications, but there is nothing like the experience of dealing with real customer network deployments.

At Blaze Networks, all our engineers have a minimum of three years working experience within the data communications industry and this is backed up with an additional minimum accreditation requirement.

Blaze Networks requires a CCNA examination pass by all our engineers. The Cisco Certificate Network Associate is an industry recognised qualification for configuring and maintaining Cisco on-premises equipment.

In addition to this we require a minimum of a Microsoft Certified Professional qualification or Microsoft Certified solutions specialist qualification meaning our entry level engineers are capable of fixing 95% of reported issues.

Our team supervisors have all of our entry level engineering certifications but additional working experience within Blaze Networks retail focused support team.

All our team supervisors and project engineers have a minimum of 5 years working experience within Blaze Networks, plus further qualifications like CCNP (Cisco Certified Network Professional) and MCSA (Microsoft Certified Systems Administrator or Microsoft Certified Systems Engineer) have been achieved.

Our consultants and core project engineers have a minimum of 10 years working experience in the communications industry and most have over 5 industry recognised certifications with 4 or more manufactures, including Cisco, Fortinet, Juniper Networks, Microsoft, IBM, NetGear, Symantec, and many more.

As mentioned, our engineers go above and beyond...

- Our recorded average phone answering time in 2018 was under 10 seconds.
- Our customer satisfaction rates recorded by closing support tickets was 97% fixed with 3% provided an acceptable temporary work around to minimise the fault impact.
- Our average ticket close time was only 10 hours across all our SLAs.

With these incredible achievements, we are confident we have the very best engineering core for your retail business.

**Q 9. Does a low set up fee, mean you have high charges for Adds, Moves and Changes?**

A 9. At Blaze Networks we currently offer:

→ 2 Year **FIXED Monthly Tariff** – so you can budget with ease!

→ **30 Day Cancellation Notice** – If you're not happy, we're not happy, so we won't hold you hostage. Plus, because we've worked in the retail industry, we recognise the need to be flexible; to be able to open "Pop-Up" stores if necessary and close stores without penalty.

Secondly, some, if not all, Moves Adds and Changes (MACs) should be included in your service contract.

If you are subscribing to a service, you should get a service. If you are doing a DIY solution, the cost from a Service Provider for MACs is not unreasonable, but we like to offer an inclusive deal. **That way you can budget with ease and still get the flexibility and support your business needs.**

**Q 10. What Service Levels should I expect to receive?**

A 10. Let me first manage your expectations!

**Here at Blaze Networks we believe we have the very best, if not unbeatable Service Level Agreements (SLAs).** We even back these up with a compensation plan if Blaze Networks does not achieve our uptime goals as specified in our retail private network contract.

**Don't be surprised therefore if you can't match these SLAs with other providers.** We pride ourselves on our network, it's resilience and the capability of our engineers.

With that said, the following explains our SLAs and what you should be looking for from a Service Provider of a private network.

Firstly, we assign priority levels to faults relating to retail locations of Critical, High, Medium, low priority and quick assist.

**"Critical"** faults are any issues relating to our core MPLS network or if over 30% of a retail estate is affected by an outage.

Our contracted SLA for critical faults is a response within 30 minutes and a fix within two hours. Failure to hit our SLA means compensation to you, our customer.



That said, **our internal target is to respond within 5 minutes** and outages of this nature should have resilience in place, meaning only a further 10 minutes is required to automatically re-terminate connectivity through alternate equipment, thus providing a very quick resolution.

**“High”** priority faults are any issues affecting more than 10% of our customer’s retail network.

Our contracted service level agreement for high priority faults is a response within 1 hour and a fix within 4 hours. Again, failure to hit our SLA means compensation, but our internal target is the same as for critical faults, thus providing a very speedy fault resolution.

***I did say our Service Levels were unbeatable!***

**“Medium”** priority is for issues affecting a single site location, but where the location has suffered complete connectivity loss.

Our contracted SLA is to respond within 1 hour and have the service issue resolved within 24 hours.

Internally however, we like to exceed expectation if possible.

We set ourselves the internal target to respond within only 5 minutes and resolve the issues within 1 hour.

In this instance, if for any reason we fail to hit our SLA, a 3G or 4G router will be **supplied free of charge** until service is restored.

**“Low priority”** is where a retail location has intermittent connectivity issues that are not affecting store trading.

Our contracted service level agreement is a response within two hours and to fix within 72 hours, but again, our internal target is to respond within only 30 minutes and to close the ticket in no more than 24 hours.

As we’ve mentioned compensation, let me explain what that means, so again you have a benchmark to aid you in selecting the best Retail MPLS network provider for you and your business needs.

In the unlikely event we do breach an SLA for critical or high priority faults, you, the customer is able to claim one day’s service credit for every connection across your entire retail estate.

We believe this is an unbeatable compensation amount but we are so confident in our network and our service engineers, that we feel that it’s not an issue to offer this level of compensation to you.

**Q 11. Is MPLS being replaced with SDWAN or is it able to lower the cost of an MPLS solution.**

I recall my first SDWAN conference call with a major network vendor, one of the big three so not to mention any names. On that conference call the technical architect stated that MPLS service could be replaced with SDWAN. In this case the provider then showed a traditional DIA (Dedicated internet service) being used to reduce load from an MPLS circuit. They were taking traffic from the MPLS line that did not need any levels of QOS and routing them over the DIA. Any high priority traffic was then routed over the MPLS line, voice in this example. The provider then said this type of layer 7 application-based routing could be used to reduce the cost of the MPLS circuit by lowering the bandwidth.

I had several issues with what was said. Firstly, our DIA circuits cost the same as an MPLS circuit so the entire example was not a good fit for us. Also, service was being re-routed, so this was no replacement of any solution. Voice traffic remained on the MPLS circuit and O365 that was just providing email was routed VIA the DIA. Why had a statement been made about SDWAN replacing MPLS?

Since this conference call I have heard many sales pitches saying SDWAN will replace MPLS and I have to say every time I investigate the SDWAN offering it is not true. Private MPLS networking does not route over the public internet therefore service providers can guarantee traffic end to end. SDWAN solutions that run over the public internet cannot apply QOS through the providers network. Actually, all the service provider can see is encrypted traffic so there is no priority level that can be added by the provider even if they wanted to. Adding QOS inside a VPN tunnel is not the same as adding QOS policies over a private connection operated by a service provider. This is because with MPLS the service provider is in full control of all equipment end to end. No one provider is in control of the public internet and all the service provider networks operating on it so building a network solely on DIA circuits would not be a good idea.

With the above said SDWAN compliments private MPLS networking with, Layer 7 routing, Zero touch provisioning, central orchestration and virtual network functions like WAN optimisation. Any IT personnel responsible for the WAN should consider adding SDWAN capability to their existing private network, as it increases security and reduces administration. However, there is a cost implication of getting these additional SDWAN benefits, and you are in most cases tied into one vendors technology stack or security fabric. Without the private network you go back to the same issues as a traditional VPN solution has and that may be ok for some organisation that do not have sensitive traffic like voice running over it, but as soon as you do or as soon as you have many branches the cost implications, security concerns and lack of control end to end will become apparent.

Blaze Networks can layer SDWAN technology on our existing private network infrastructure providing our customers with all the benefits of SDWAN whilst retaining control of traffic end to end. To learn more about SDWAN ask for our SDWAN

solutions brief or do not hesitate to call us for more detail on available SDWAN solutions.

**Q 12. *Is SDWAN more cost effective.***

***Unfortunately, true SDWAN is not more cost effective. SDWAN comes with a lot of benefits, a true SDWAN consists of;***

- 1. Multiple Active Paths*
- 2. Any Transport Technology*
- 3. Application aware Routing*
- 4. Zero Touch Provisioning*
- 5. Centralised Control / Orchestration.*
- 6. Central Monitoring*
- 7. Virtual Network Functions, like WAN optimisation and security.*

The downside of adding functionality is the increase in cost. If you run an SDWAN network over all unmanaged cheap DIA services, then you could reduce costs but would impact your control of the solution end to end. The fact that you are using unmanaged cheap DIA circuits means you are taking on the responsibility to monitor and correct faults, something better left with a service provider. We have seen some IT personnel taking this responsibility back on without understanding the true impact.

I trust you find this set of Question and Answers useful. If you have any other questions, please don't hesitate to contact me on 01625 506778

## Blaze Networks Testimonials

*“Proactive, reliable and fast are words I would use to describe the service I get from Blaze Networks’ Retail MPLS Network. I especially like the capability of automatic notifications from Blaze Networks monitoring platform that prompts me in real time when connectivity is down.*

*This allows me to easily maintain all our SQL database links across my entire retail estate. I’ve also made huge savings in both time and money through having a single point of contact”*

Keith Slide  
IT Director, Litecraft (Cascade Holdings Limited)

---

*“Blaze Networks’ Retail MPLS Network is incredibly good value for money. Outages are very rare, but if they do occur, Blaze proactively contact the store and fix the issue usually before I’m even been made aware of it, meaning we experience very little downtime.*

*Would recommend to anybody in the retail industry.”*

Iris O’Neill  
IT Manager, Menarys

---

*“Blaze Networks’ Retail MPLS Network has provided us with a very resilient branch infrastructure, enabling us to provide a great service to our customers.*

*They proactively contact stores and fix any issue before it becomes business impacting. Excellent company to work with who truly understand our industry and business requirements.”*

Chris Marchant  
Company Secretary, Collectables Retail

---

*“The Retail MPLS Network from Blaze Networks is incredibly fault tolerant providing 100% uptime for our business.*

*In addition to the usual store traffic, we stream real time CCTV video 24/7 and have never been hit for an “Over Use Charge” like other vendors do.*

*Their support team always goes over and above what’s expected. Having just one company to deal with for our entire WAN solution has made my life so much easier. I have 100% confidence in Blaze Networks and their Retail specific solutions.”*

Adam Sheffield  
IT Manager Wilton and Bradley

Here's an AMAZING OFFER we've put together.

You can now get a brand new Fully Managed Private Network or Private SDWAN enable network for your retail business, including as many locations as you need, with...

- 2 Year **FIXED Monthly Tariff** – so you can budget with ease!
- **30 Day Cancellation** Notice – If you're not happy, we're not happy.

I worked for a retail business for 5 years as their Head of IT. I know how important it is to ensure a Retail Branch is secure, compliant and can make transactions at all times; especially in peak shopping periods.

That is why I joined my brother at Blaze Networks to develop the Network I would have wanted when I walked in your shoes.

**Call Me on my direct line, 01625 506778, to claim this amazing offer!**

If You're Looking to...



- + Save Money
- + Reduce administration and complexity
- + Improve PCI DSS Compliance and/or simply
- + Expand or grow your network...

...don't do anything until you've spoken to us. Our network was designed for businesses like yours in the Retail sector.

## 10 Reasons to Choose our Retail Private MPLS Network

1. Fully Managed with Advanced Proactive Network Monitoring
2. 99.99% Core Uptime Service Level Guarantees
3. High Performance/Bandwidth Availability – No “Fair Usage” restriction; Truly Unlimited
4. Flexible 30 Day Contracts – Ideal for seasonal “Pop-Up” Stores or Store Closures
5. Simplified PCI DSS Compliance – Whilst reducing Pen. Test Costs
6. Free Consultancy – Sharing our experience of Moves, Adds and Changes
7. ITIL Framework – Our network operations centre follows the ITIL framework.
8. Price 2 Certified Project Management Team – to make life easier
9. Ideal for Businesses Migrating From Expensive VPN Deployments
10. Built Specifically to Meet the Needs of Retailers like you

**Call me now on 01625 506778 to discuss  
your network requirements.**