WHITEPAPER

Wide Area Networks - the wider issues

Five new concerns when choosing a WAN

www.colt.net

Contents

Introduction

In an IT world where the pace of change rarely slows, owners and providers of Wide Area Networks (WANs) may be forgiven for thinking that they live in a relatively calm part of that world.

It may seem that after the transitions from analogue to digital networks, with their litany of jargon abbreviations (PSS, IP, MLPS etc) and Cloud constructs, the fundamentals of Multi-Site Networks have not changed. But this is an illusion – certainly in terms of functionality but also in the emergence of new operational capabilities and requirements need to change to meet new fundamentals.

In this White Paper we highlight some of the criteria and developments you should include in any requirements documents you are producing:

- **essential design criteria for IT professionals considering WAN design,**
- **significant WAN developments driving this change,**
- **potential impacts on the wider enterprise.**

The traditional approach to design, when there were fewer connectivity choices, tried to balance performance and cost. In many countries the connectivity options now include diverse broadband technologies and dedicated circuits including dark fibre. The broadband options may include, ADSL, Cable/Copper with Fibre to the Cabinet (FTTC) or Fibre to the Premises (FTTP) - but designers must be aware of their characteristics.

- Will the site location be impacted by signal degradation of FTTC (VDSL) on account of route length from the serving cabinet?
- Are asymmetric services suited to the site's applications systems or should higher regard be given to upload performance?
- Is the site's operation likely to be impacted by high contention at specific times?
- How important is latency for efficient transaction systems?
- Can the provider provide assurances on maximum packet loss?

For smaller offices in well-served locations, broadband services could be a suitable solution – particularly if there is no local operational concern for circuit protection, diverse routing or back-up capabilities. If, however, uptime is important, does the provider offer a backup solution via another medium? With increasing 4G coverage with higher data (download) transmission rates, this medium may be practical as a backup, temporary, emergency or a low cost solution, helping to fulfil more stringent service level demands.

Given these constraints and options, it is no surprise that there is no such thing as a completely standard WAN – each must be crafted to meet the current and future needs of the specific business. Successful network design will have a major impact on productivity and can be crucial in opening up opportunities for digital business development. On the other hand, an inadequate network – designed perhaps for the needs envisaged a decade or more ago – will inhibit productive work and cause employees, suppliers and (indirectly) customers considerable frustration.

Beyond connectivity, what other criteria must feed into a Multi-Site Network design and the outline investment case that will play a key role in future Request for Proposals?

Don't forget the five wider criteria

Matching business growth

Mapping out requirements will obviously start with the enterprise geography and demography and include consideration of enterprise growth patterns.

Growth may be organic within the current estate or more acquisitive – suggesting that great emphasis must be placed on the ease and speed of future integrations.

Fundamental questions need to be asked about employment trends and the roles of supplies and/or marketing channel partners – and on the strategic responses to those questions will hinge the scope for future agility and adaptation to new business models. And don’t be surprised if the answer is; “we don’t know yet”. However, the more rigour and testing of assumptions that can be done at this stage, the more robust the final design will be – and the easier it will be to iterate by going back and testing the origin assumptions were based.

There is, however, no doubt that the diverse options for mixing and matching Virtual Private Networks, the Public Internet, dedicated private networks and Cloud services allows for a more rapid response to changing growth requirements.

> “And don't be surprised if the answer is: "we don't know yet"”

Security

> **The selection of security options rests on the applications you are providing to the end users and the way they have to be accessed**

As the plan takes shape, questions of security and associated risks will play a continuous part. There may be good commercial reasons to use the shift into to a more digital economy, to break down long-standing silos within an enterprise and ensure that data flows more freely. However, compliance with internal and external information security policies must be maintained to ensure the reputation and operation of the business is maintained.

New security issues are being raised by the shifting pattern of user devices – and particularly the increasing use of mobiles and access via the public Internet. With frequent software updates to apps and browsers, a traditional solution such as SSL may now seem less convenient – or indeed positively dangerous. Web-based SSL is included in everyday browsers and there are fewer things a user needs to do to configure access to the network. However, after each browser update, connection to the WAN may need to be postponed until the new version is checked and validated. Concerns may also be raised about Trojan Horses and other vulnerabilities (like Heartbleed and Freak) that may be present in Open SSL and allow hackers to steal supposedly protected information.

The alternative – the tunnel-based access protocol IPsec - is a topic which may best be explored at the RFI stage with potential service providers. Designers may consider offsetting initial installation complexity to deliver advantages of browser-agnostic updates (eliminating the maintenance workload and lowering risk) or find it more important to have encryption for file-sharing and VOIP calls via the Internet.

The selection of security options ultimately rests on the applications you are providing to the end users and the way they have to be accessed. If everything is web based or run via virtual desktop, then SSL would be the first place to start. For proprietary applications, file sharing between end machine and servers, and technologies like VoIP, then a dedicated encrypted tunnel may be needed: IPsec in this case being the more appropriate choice.

Cloud considerations

Businesses are increasingly attracted to offload a range of processing and storage requirements to Cloud Services providers.

The attractions are fairly obvious in theory – a more easily expandable capability, far less in-house routine systems maintenance and greater scope to focus on new developments that will impact the bottom line more by growth than through cost-cutting measures. There is no shortage of providers.

Many are accessed only via the Public Internet and not all offer scope for a dedicated link from your own WAN – a fairly vital capability if your design is not to be dependent on the potential vagaries of Internet access.

Direct linkage to Cloud-based systems also enables you to better balance your network traffic by tracking which traffic goes to the cloud service and which stays on internal networks. The changing balance of this traffic between in-house and cloud services will also give some valuable insight into changing business priorities.

> “Expandable capability, far less in-house routine maintenance and scope to focus on new developments”

Balancing In-House WAN Design versus External Provision

Again, in theory, an in-house design and build project for the WAN would provide the greatest control over your infrastructure. x\But providers will point to the complexities of licence management and circuit leasing as (a) unnecessary distractions from higher priorities and (b) their greater scope for adapting the design as business requirements change over time.

Choosing the most suitable WAN provider is a challenge but it is often the case that organisations and service providers that have already trodden this path will be happy to share their experiences. Those conversations will almost certainly feed into the design debate around network topologies (Stars, Hubs or Fully-Meshed) and the traffic loading expected from different sites. Enterprises that already utilise a WAN may have an advantage during redesign on account of better traffic metrics though this will not always extend to sites not previously included.

Here again, every enterprise will have differing requirements – so a key capability of a supplier is the strength of their network planning expertise. There is now a huge variety of access solutions including various levels of broadband capability and leased lines (Ethernet) for heavy duty links.

We would recommend taking a very good look at the needs per site. For the bandwidth hungry sites (data centres, headquarters, and other large sites) - large Ethernet based connections should be considered. Include in this the installation and management of all routers and switches that are needed to connect the Ethernet based solution to any other IP based service.

MPLS based VPN can be used to connect the data centre to the medium sized sites, that need Quality of Service, high availability connectivity, and security. And with the really small sites and the sites that are not data hungry consider an Internet based VPN.

The really small sites could be Internet based on terrestrial lines, but why not base it on mobile internet? Make sure the service provider is at least capable of offering this option.

With a gradual improvement in mobile technologies it may be entirely possible to service small sites or individuals via 4G services – but care is needed to check out coverage patterns. This may be a very important issue if sensors (e.g. for tracking mobile assets or monitoring of remote production resources) are an important part of systems input.

> **“Choosing the most suitable WAN provider is a challenge but many organisations and service providers are happy to share their expierences”**

Looking Ahead - software-defined everything

Software Defined Networking (SDN) and Network Functions Virtualization (NFV) in the WAN are at the forefront of network development.

Networks have always comprised two elements – the physical connection and its terminating router. That router has previously been a device dedicated to a specific use – and needs replacement and/or reconfiguration when requirements change.

By decoupling the hardware element from the control functionality it is possible to offer Software Defined Networking (SDN) or, as providers would say, Network Functions Virtualization (NFV). The concept has already been deployed within Data Centre's internal networks and will almost certainly now become a feature of managed WAN designs.

In one sense this will ease planning by allowing greater flexibility for future upgrading and, particularly for dynamic event-driven environments, allow for different parts of the network to be scaled up or down. Early experience with SDN has shown the value of point and click self-service portals for end-user ordering of additional functionality at short notice – e.g. the need to switch on extra capacity for a major customer event or a development team's need for intensive testing. Even household customers could enjoy the flexibility to temporarily boost their broadband from 100Mb/s to 1Gibabit/sec when their teenagers' friends arrive for to download the latest multi-user online game!

It is therefore advisable, when considering WAN renewal to explore the extent of potential suppliers' expertise in this significant arena.

> “Take a very good look at your needs per site and explore the extent of potential supplier's expertise”

To the future and beyond

In this brief overview of the multi-site networking landscape we have touched on the basic planning issues and considered growth issues, security, cloud connectivity and the balance between in-house management and external provision.

We have also looked ahead to the emergence of SDN/NFV capabilities and the flexibility they will eventually provide for matching network capacities to the ever-changing needs of the enterprise.

It is clear that multi-site, multi-device networks that are easier to manage will ease IT professionals' maintenance burdens and allow greater time to focus on the strategic/priority needs of the enterprises. However, you need to ask the right questions - and to ask them to the right service provider.

> “Easier to manage multi-site networks will allow greater time to focus on the strategic priority needs of the enterprise.
>
> However, you need to ask the right questions to the right service provider.”

About Colt

Colt provides network, voice, and data centre services to thousands of businesses around the world, allowing them to focus on delivering their business goals instead of the underlying infrastructure. Customers include 18 of the top 25 bank and diversified financial groups and 19 out of the top 25 companies in both global media and telecoms industries (Forbes 2000 list, 2014). In addition, Colt works with over 50 exchange venues and 13 European central banks.

Colt operates across Europe, Asia and North America with connections into over 200 cities globally. It recently completed the acquisition of KVH – which now operates under the Colt brand - an integrated data centre and communications services business, with headquarters in Tokyo and operations in Hong Kong, Seoul and Singapore.

www.colt.net

COLT

www.colt.net I @colt_technology I info@colt.net

Share this document

colt