26 August 2016

Managing WANs in MNC Enterprises

Assignment Report

Course: Computer Networks (CO300)

Degree / Semester: B.Tech. / Fifth

Department: Computer Science and Engineering

Submitted by

S.No	Reg. No	Name	Signature
1.	14CO202	Pranathi Alla	
2.	14CO203	Anirudh Sriram	
3.	14CO204	Aparna R Joshi	

4.	14CO205	Bairi Sandhya Rani	
5.	14CO206	C.B.Yuvaraj	
6.	14CO207	Chiranjeevi AR Hegde	
7.	14CO208	Deepak Srikanth	
8.	14CO209	D.Teja Sri	

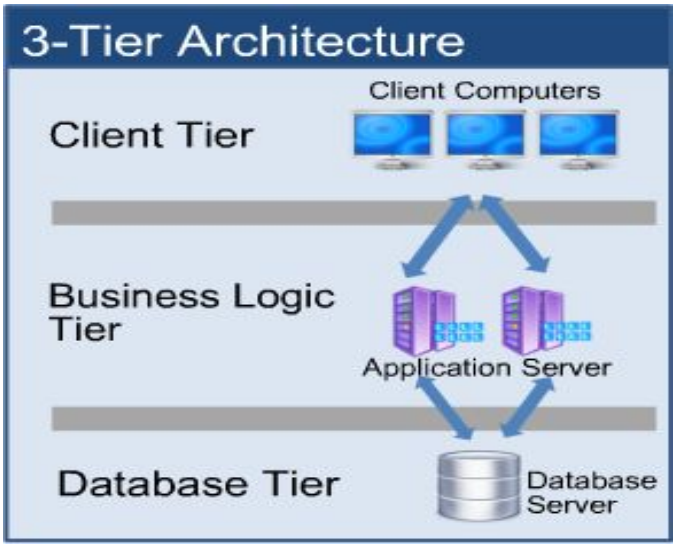
Table of Contents

Managing WANs in MNC Enterprises

1. Business Case

The objective of the project is to analyse the current network architecture being implemented in the organization for all the tiers in the CISCO WAN architecture model because the chosen organisation confirms to three-tier-WAN architecture and this architecture constructed with dedicated facilities offers even greater fault tolerance and scalability.

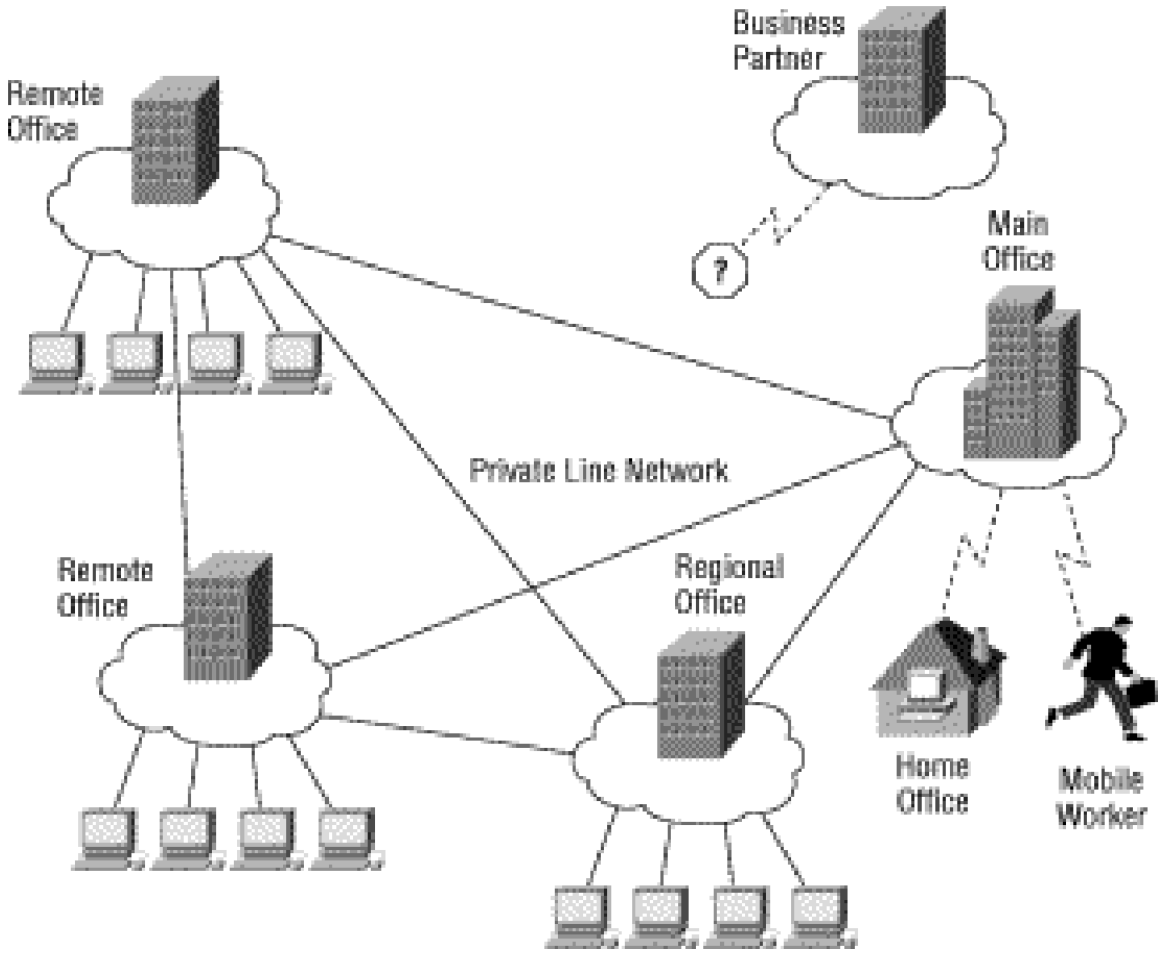
The project also aims at making recommendations for the different network models that can be implemented in different tiers of the three-tier architecture.



Globalisation is an aspect that any good company hopes to aspire. A Multinational enterprise that has already attained global reach prioritizes to maintain network efficiency. In this aspect, organisations face unique challenges when it comes to managing their WANs.

To successfully deliver consistent end user experience across geographies, close WAN integration will also be important. Many multinational corporations (MNCs) self-manage their IP telephony, video conferencing, and UC(unified communication) solutions today, but as the complexity of networks grows with the adoption of these newer communications applications,

achieving performance and cost efficiencies while adopting and managing performance-sensitive applications becomes a challenge.



Network designers in the organisation have two options to increase the efficiency levels of the network: either increase MPLS bandwidth, which is cost prohibitive, or supplement MPLS with Internet-based connectivity. Since the Internet is an untrusted WAN transport, using it as part of a corporate backbone requires a lot of planning to secure dynamic connectivity. In many cases, retail and financial institutions have deployed separate networks with local Internet exit to offload certain traffic.

1.1. Current State Summary

In the current scenario of the organization, MPLS is being incorporated in the Database tier and the client tiers in the WAN architecture, but communication among data centers using MPLS did not result in the efficiency expected, whereas in the client tier a simpler cost effective networking architecture will be better suited.

Surprisingly, though MPLS has many advantages like built in support for QoS(Quality of Service), service level agreements with delivery guarantees and outsourced routing, the most common use for MPLS is to connect branch offices to data centers and interconnect branch offices to each other i.e, in the business logic tier in the WAN architecture.

1.2. Opportunities

The opportunities existing in today's world include the traditional carrier Ethernet to interconnect the data centers in Tier 1. The downside to this is that carrier Ethernet services don't scale to the same order of magnitude of sites as MPLS. Because MPLS is a routed network, it can support tens of thousands of sites or even more. Carrier Ethernet, in contrast, is effectively a giant bridged network, which can not scale easily beyond a few hundred sites.

Clearly, an alternative has to be sorted out to be incorporated in the database tier and client tier as well as to achieve better performance.

2. Communication / Networking Requirements

The multinational IT companies operate in many countries and these companies must reconcile different services from different service providers. For example, most IP VPNs are based on MPLS technology that cannot easily extend beyond each carrier's network. Over the past several years, consumers have declared their desire for new services and products that include things like video teleconferencing, podcasts and IP phones with wireless access which is an important customer requirement.

Some other customer requirements include Convergence (voice, video and data with a single backbone connection), Segmentation and Security, Availability/Redundancy, Scalability, Adaptability, Cost and Control.

Any IT MNC requires building a WAN that can accommodate dynamic, arbitrary topologies and a fluid data plane across any kind of transport (Internet, MPLS, LTE, etc.) requires a policy-driven infrastructure.

Other than the requirements of an MNC for an efficient transfer of data among the different branches, the corporate company has several requirements, which include business and technical requirements.

- To support new and maturing international business operations, corporate IT needs a reliable and robust wide area network (WAN) connecting major operational sites and those running critical applications with regional or global data centers and among larger sites and headquarters.
- IT must also ensure consistent application performance across geographic regions, including 24x7 remote IT support.
- Another strong requirement is the company's ability to install new services quickly, benefit from lower-cost new technologies, and apply flexible bandwidth options for different site sizes and types.
- The company needs to optimise broadcast traffic, and efficient network bandwidth management and utilization.
- Seamless global coverage MPLS platform enabling identical services at any business site, regardless of location.
- The MNC should be able to have a full control of network traffic; ensure the availability of bandwidth for critical applications and increase network efficiency and reduce traffic congestion.[1]
- Among the most important factors when integrating different technologies in a large MNC's WAN are the ability to use the same access link for voice and data traffic and to easily and quickly increase connectivity capacity as needed.
- Highest reliability, agility, visibility and simplicity for connecting a global enterprise's complex and highly distributed ecosystem of employees, customers and partners.

On service provider side, a single MPLS, Internet or LTE can offer secure transport, complete path diversity, detect congestion, failure, loss and latency in the data plane. Furthermore, this application-aware path selection approach provides virtual quality of service without forcing all carriers to honor marking across peering locations.

Quality of Service prioritizations is a key requirement of MPLS kind of solutions that helps ensure that users worldwide have a consistent experience using performance-sensitive applications such as VoIP, unified communication(UC) and telepresence.

Most firms require a combination of MPLS, carrier ethernet and Internet VPNs that can outsource some or all of their WAN. Single sourcing global MPLS IP VPNs appeals to majority of MNCs.

MPLS and VPLS services offer fantastic scalable and fractional bandwidth with 100Mbps Ethernet as the standard with a high prevalence of 1Gbps Ethernet circuits. Support, agility, performance, resiliency, adds / changes, application QoS, migration, service management and must be capable of meeting the organization's unique business needs.

These global WANs also require removing computationally intensive operations from every router that can help in extending the data plane life of these devices.

Some of the technical requirements for the transfer of data across the wide area network connecting the MNC include:

- Minimization of packet loss
- Minimization of delay
- Maximization of throughput
- Enforcement of Service Level Agreements (SLAs)

3. Networking Challenges

We may encounter certain problems while carrying out VPN migration and support.When considering migration, the regulations which exist within each region may impact the delivery of services. In addition, time zones, local language, access restrictions, bandwidth availability and local IT capability all conspire against an organisation to ensure global WAN provision remains a challenge. The MPLS scheme depends entirely upon a single carrier network. This could be thought of as a single point of failure, i.e. the entire system could be down as a result of a failure on the part of the service providers.

The MPLS system adds an extra layer to the network that sits between the 2nd and 3rd layers of the OSI layered architecture. Although no physical changes need to be made, an MPLS network on such a large scale (for an MNC, that is) needs LERs and LSRs (Label Edge Routers and Label Switch Routers) to implement the new routing protocols, which the means that lots of routers need to be reconfigured to be able to work with MPLS.

MPLS works by prefixing packets with an MPLS header, containing one or more labels, called the label stack. While the label stack concept provides some benefits, the number of labels is likely to increase the overhead, certainly in terms of making the MPLS header larger.

At its basics, MPLS is a traffic routing mechanism and so offers no inherent data protection over the network. No data is encrypted within MPLS and hence any attacker with either logical or physical access to the network core can access all data sent over the network. Improper implementation or configuration of the MLPS system can open up the system to such vulnerabilities.

Overall, the procurement of global networks, multi protocol label switching is perhaps more challenging vs national provisioning for the reasons stated above.

4. Networking Solutions

1.Carrier Ethernet

One of the alternative for MPLS is carrier ethernet. It is cost effective and also easy to connect remote areas.Carrier Ethernet is on its way to becoming the service providers' technology of choice due to its combination of improved revenues, better cost management and opportunity to lead customers into the managed services space.

Advantages of using carrier Ethernet

- Ethernet is typically more affordable than MPLS.
- Ethernet gives WAN engineers control and responsibility over routing.
- Ethernet offers low-latency and high-throughput, which is ideal for disaster recovery.
- Unlike MPLS Ethernet exchanges have made Ethernet WAN services available in more locations.

Disadvantages of carrier ethernet

- Not suitable if number of sites to be connected is very large.
- Carrier ethernet networks can offer interoperability challenges between carriers.

2.Software Defined WAN (SDN)

Software-defined networking (SDN) is an approach to computer networking that allows network administrator to manage network services through abstraction of lower-level functionality. SDN is meant to address the fact that the static architecture of traditional networks doesn't support the dynamic, scalable computing and storage needs of more modern computing environments such as data centers.

- SDN architecture is directly programmable , agile , centrally managed.It is a better alternative to MPLS and carrier ethernet.

Advantages of using SDN

- SDN allows IT managers to experiment with network configuration without impacting the network. SDN also supports management of both physical and virtual switches and network devices from a central controller.
- The SDN Controller provides a central point of control to distribute security and policy information consistently throughout the enterprise.
- SDN should lower overall operating costs and result in administrative savings.
- It offers better Quality of Service.
- Open networking is about providing choice and design options, making networks responsive to IT requirements and lowering overall costs. Technology vendors are responding to IT customer requirements with a wide range of products that enable open networking.

Why Open Networking?

Networking across the data center, campus, and wide area network (WAN) is now a key inhibitor to IT innovation. Network services, including Ethernet switches, routers, security, and Layer 4-7 appliances, are traditionally delivered in highly optimized, proprietary combinations of hardware and software (i.e.boxes).
Today's installed (closed) networks have the following disadvantages to IT organizations:

- High OPEX and CAPEX costs
- Limited flexibility, agility, and automation
- Lack of seamless interoperability between vendors
- Limited-to-no automation
- Slow network deployment
- Static network architectures where scaling normally equates to CAPEX expense via additional network devices and/or higher bandwidth ports are needed
- Closed proprietary systems that promote vendor lock-in and inhibit open programmability
- Slow rate of innovation
- Lack of visibility, monitoring efficiency, and useful analytics
- Lack of accessibility to IT operations and management teams

- Less flow predictability due to randomized distribution of workloads across compute and storage coupled with application traffic flows shifting from north-south to east-west
- Open networking, which decouples networking software and hardware, has the potential to alleviate many of these pain points. Open networking offers the flexibility to choose from a variety of network hardware (e.g. servers and white box switches) and network operating systems. Open networking provides the platform to drive innovation and enable a broad ISV ecosystem. The benefits of open networking include:
- CAPEX relief via hardware commoditization.
- Ability to run network operating systems with close ties to IT platforms (e.g. Linux)
- Automation of compute, network, and storage thanks to a common set of management tools that span all three areas
- Ability to choose from a variety of network applications (and the flexibility to develop new applications)
- Multi vendor, interoperable network architectures that are defined by IT architects versus vendors

Leading IT organizations describe their wide area networks, including branch office networks, as static, fixed, inflexible, and costly, which can impact the business' bottom line. These organizations are frustrated by their inability to rapidly adapt their WAN to accommodate the significant changes in traffic patterns brought by increased adoption of mobile and cloud computing. Branch office employees need access to public and private cloud-hosted applications over the WAN, but security concerns and the inability to use the WAN as a flexible resource pool has caused traffic flows to become inefficient.

- The majority of the leading IT organizations are starting to implement open networking. We are at the beginning of a long term networking industry transition into a more software-oriented, standards-based structure that promises to provide significant benefits to the IT community.
- As described above The pain points in branch office networking are many. We anticipate that SD-WAN deployments will accelerate rapidly as branch office networking responsibility and budget control often resides within a single group. While there is much interest in SD-WAN, the innovative technology and the vendors offering solutions are in the early stages of implementation thus, time is required for vetting.

5. References

[1] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.3038&rep=rep1&type=pdf

[2] http://searchnetworking.techtarget.com/blog/The-Network-Hub/Challenges-of-Global-MPLS-Network-Procurement

[3] https://www.business.att.com/content/whitepaper/ATT_TyingWANLANtoIPVPN.pdf
[4] http://www.networkworld.com/article/2942631/infrastructure-management/managing-global-wans-in-multinational-enterprises.html
[5] http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml#wp28489
[6] http://www.rcrwireless.com/20140513/wireless/mpls-security
[7] http://searchenterprisewan.techtarget.com/tip/MPLS-advantages-and-disadvantages-for-WAN-connectivity
[8] http://www.networkworld.com/article/2942631/infrastructure-management/managing-global-wans-in-multinational-enterprises.html