Journal of Engineering and Applied Sciences 13 (22): 9651-9655, 2018
ISSN: 1816-949X

Direct Cloud Connectivity and Increased Bandwidth

Mustafa Abdalrassual Jassim
College of Engineering, Muthanna University, Samawa, Muthanna, Iraq

Abstract: This study is about learning how the direct cloud network connects to lower costs, increases bandwidth and delivers more consistent network performance. This study describes the driving factors behind network expansion requirements and discusses the architectural options to expand the data center connectivity in a cost-effective manner. This study also shows the business benefits of creating a dedicated network of customization facilities for the general cloud provider. Data centers have become inextricably linked to the cloud for many organizations and in all sizes. Communication has become more important as a broad application. To maintain data, confidentiality, reliability and transmission speed, more data transfer and network expansion were used to ensure faster response, increased productivity and a more consistent network and bandwidth.

Key words: Bandwidth, cloud connectivity, architecture, data center, productivity, broad application

INTRODUCTION

Computing technology has been evolved over the years. There have been steady developments in the field of computing hardware, software architecture, web technology and network communication over the last decade (Hamid and Yusof, 2016) cloud computing enhances its low cost and simplicity for both service providers and users. Cloud computing plans to take advantage of multitasking by serving multiple heterogeneous applications simultaneously (Cai *et al*., 2015). Cloud computing is a web-based computing model that offers a lot of services such as on-demand (Qi *et al*., 2014) bandwidth. It represents the size and time and represents the amount of data that can be transferred between two points at specific time intervals. It is sometimes expressed as bytes. It indicates the data rate supported by the network connection or interfaces connected to the network. Bandwidth should not be confused with through put which refers to speed. While high-bandwidth networks are often fast, that is not always the case (Manzano *et al*., 2013). Providing of information technology services such as software, storage, network, hardware and other resources is delivereded to the client through the network (Khan and Tuteja, 2015). This study discussed the driving factors behind network expansion requirements and architectural options for extending data center connectivity in a cost-effective and operational way. Datacenters have become inextricably linked to the cloud for organizations of all sizes. There are reliability and security issues associated with basic internet connections. Direct cloud connectivity establishes a dedicated network connection from a colocation facility to any cloud provider, increases bandwidth productivity, reduces network costsand provides a more consistent network of Internet-based communications. In addition, this study highlights the role of standards to improve the privacy and security of cloud computing and identifies areas where future standardization can be effective."Direct connect" is viewed as an essential tool for consistent, cost-effective and secure operations (Fig. 1 and 2).

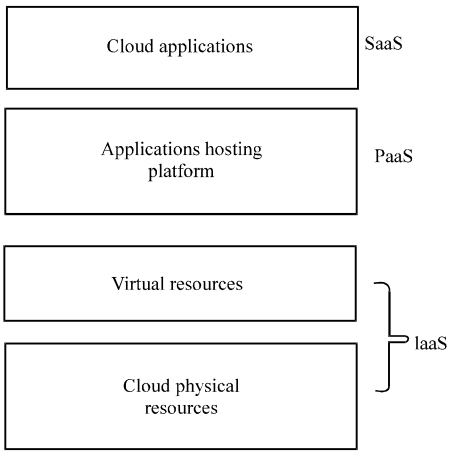

Fig. 1: Cloud computing layers

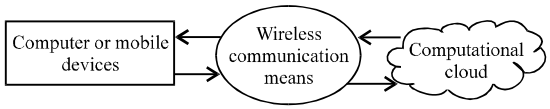

Fig. 2: General view of comutational cloud

How to increase the hosting bandwidth with virtualization of the data center? The main reason for increased availability of bandwidth with virtual data centers lies in the common nature of serversit self (Hawramani, 2017) because each device is connected to one physical server and shares the capabilities of this server. You can remove multiple servers with traffic and install the application and the result will lead to increased bandwidth. In addition, the server virtualization does automatically reduce the bottlenecks in the input and output traffic to facilitate the flow and increase speed. Eliminating bottlenecks gives servers the ability to better utilize bandwidth and get more to their current levels. Finally, current and automatic traffic analysis tools prevent network overloads and replace failures by providing long-term usage expectations.These expectations give business owners the ability to predict future traffic flow before it creates a bottleneck. Thus, a vast amount of data is processed in parallel with large groups of nodes in a reliable manner (Fig. 3):

- Each leaf connects to all spines in the network
- The spines are not interconnected with each other
- The leafs are not interconnected with each other for data-plane purposes

The change information will be transferred differently to and after the link state protocols when a change in the network topology occurs and must be transferred to the rest of the network with the local guidance system (Fig. 4).

Each router learns the entire network topology through exchanging information with all other routers. Itthen calculates the least-cost path to the other routers. "The number of times the loops are executed is equal to the number of nodes in the network", taking into account the following:

- Flood topology change information
- Each router calculates the new best path independently
- Link state
- Topology change
- Router A-C
- Calculate best path and send information to router (B)
- Calculate best path and send information to router (C)
- Calculate best path
- Distance vector

Figure 5 illustrate show router 1 finds the distance to other routers in the network.

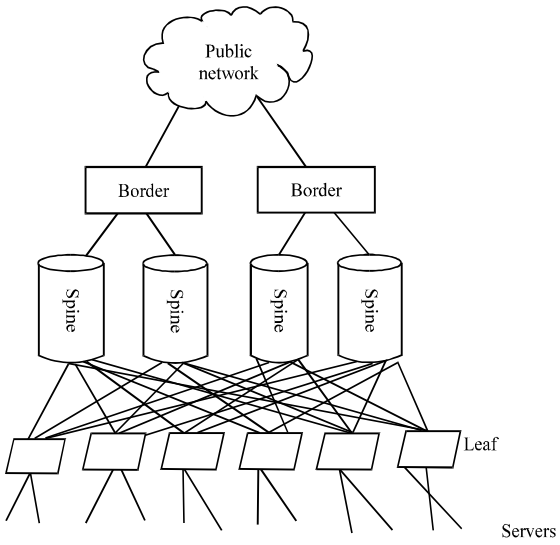

Fig. 3: The spine leaf topology

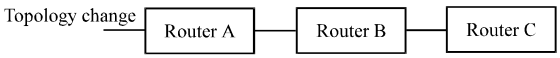

Fig. 4: Linking distances

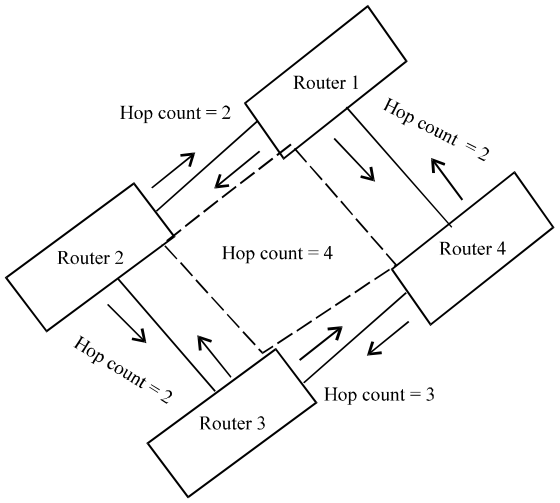

Fig. 5: Distance to routers

Why direct connect?

- Predictable and reliable performance to your AWS cloud
- Enabling of new services and applications
- Increase security through private connectivity
- Reduce network costs by avoiding internet bandwidth and bandwidth charges
- Increase performance by bypassing congestions

Algorithm 1; Router management system:
Input: Information from the datacenter network
Output: Flow mechanism and link utilization update
1: Receive information
2: Spine router controller
3: Case spine router ID to activate/deactivate
4: Find router
5: If (requested.destination is outside datacenter)
6: Find network information
a: Update for links
b: Network Monitor
7: Else Network Information
a: Routing
8: Send the flow route and link utilization increase update
9: Flow Routes
10: Activate/deactivate spine switch
11: Datacenter Network (Spine Leaf Topology)
a: Traffic Request
b: Network Information

The security of direct cloud connectivity: Now that the use of cloud computing in the last period has increased rapidly, the security situation of cloud computing is considered the main issue in the cloud-computing environment. The distance between the client and the physical location of his data creates a barrier because this data can be accessed by a third party and this would affect the privacy of the client's data (Sivasankari and Sivasankaran, 2015). Decisions on the adoption of cloud computing (Mink, 2015), resource management and service delivery (Subashini and Kavitha, 2011; Garrison *et al*., 2015), distributed Denial of service attacks (Nelson, 2015; Singh *et al*., 2017), fatal attacks (Osanaiye *et al*., 2016), cloud-based security learning (Somani *et al*., 2017) threat and risk systems (Kar and Mishra, 2016) an integrated model for dealing with cloud incidents and forensics (Ab Rahman *et al*., 2017), a cross-tenant access control model (Alam *et al*., 2017) and so on. In addition, data leakage causes many problems for cloud computing users. The purpose of this research is to deal with security risk, develop appropriate solutions and avoid problems.To ensure that cloud storage and security are secured, it must be encrypted where data is transferred across networks and stored in databases. By using encryption, the information is protected from anyone who is not authorized to display your data orit gets less accessible by the hackers. As an additional security measure, different security settings can be set to the cloud; based on the user. Before implementing encryption, the organization needs to ensure access to the database andto control its components and processing by authorized users as well as allowing users to access the objects and permissions of users to perform various commands and tasks. The following graph (Fig. 6 and 7) shows how access control and encryption reseach together to secure data.

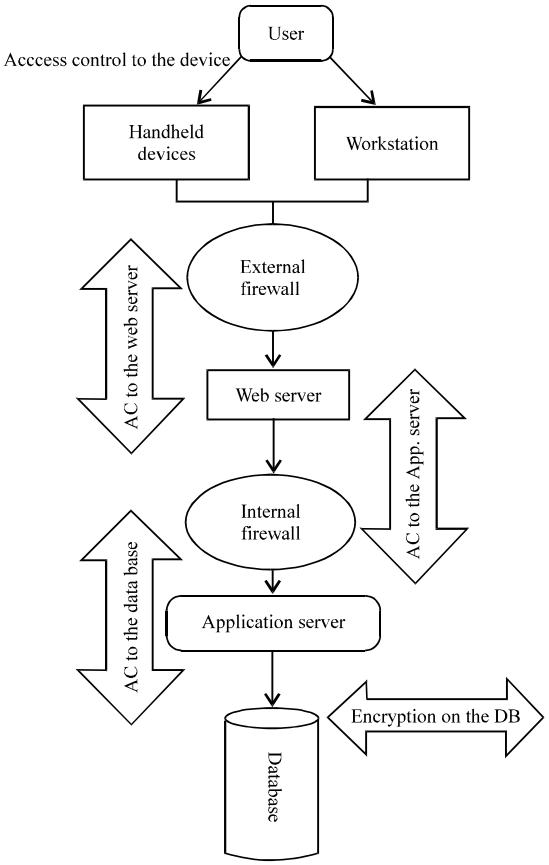

Fig. 6: Data motion

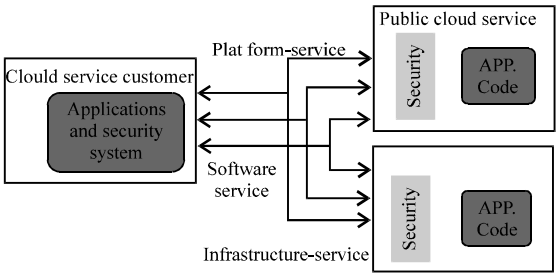

Fig. 7: Components and connections for cloud computing

We provided some steps to be taken into consideration to ensure the deployment of cloud computing by a cloud service client. It takes into account the differences that result from the IT level and the size of the organization. Several steps are discussed including:

- Define the cloud deployment model for data and applications
- Integration with existing enterprise services
- Addressing communication requirements
- Development of service agreements and governance policies

- Evaluate and resolve security and privacy challenges
- Manage the cloud environment
- Consider the plan for archiving, backup and disaster recovery

It is useful to take into account the image of the components and interconnections involved in cloud computingas shown in Fig. 8. This divides the components that are of interest to the cloud service client into three groups-the client's internal systems, the components that operate in the private cloud services or outside buildings and components that operate in public cloud services. Figure 8 also highlights three types of interfaces between these groups-the business interfaces used to manage subscriptions, the administrative interfaces used to manage and control applications and services (this includes security management) and the functional interfaces of applications and services, invoices and payments. The internal customer systems are divided into internal applications, administrative applications and security systemsas well as internal data sets and databases. For both cloud and cloud services, the main components described include the application code ("for applications running within the cloud service") with their application environment, cloud service client data and data from cloud services (including records). The main concern of mixed cloud deployment is to ensure the effective and efficient integration of all components in the 3 groups in Fig. 8, taking into account interfaces between them.

The benefits of direct cloud connectivity: For end users, direct cloud connectivity can be simple and secure. Thebusinessbenefits include:

Reduced bandwidth costs: For bandwidth-heavy workloads running on the cloud,direct cloud connectivity reduces network costs into and out of the cloud in two ways:

- Companies can reduce the bandwidth of the internet service provider by transferring data to and from the cloud provider directly
- Data are downloaded through dedicated connections less than Internet data transfer rate
- Consistent network performance. Given that the internet is constantly changing

The flexibility and ability to scale on a moment's notice lowers risk and operationalcosts while increasing agility. IT also is simplified when using one point of contact forall cloud and internet services, eliminating

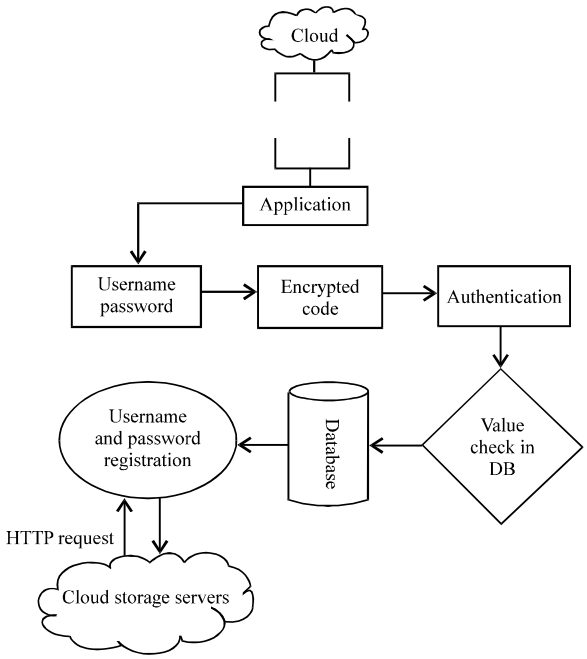

Fig. 8: Proposed system

conflicting services and contracts. It's alsoeasier for businesses to maintain robust communication with end users when theycan provide a unified set of services across many well-integrated platforms. A private network is a solid and good tool for organizations that have a large deployment and are based on another site or perhaps a storage capacity or a premise for increasing information technology while taking advantage of the cost and performance benefits of dedicated point-to-point communications connections.

Conventional data center network topology:

- Internet
- Core Layer (CL)
- Core Router (CR)
- Aggregation Layer (AL)
- Aggregation Switch (AS)
- Access Layer
- Top-of-Rack Switch (ToR)
- Servers

Factors affecting WAN: The most important factors affecting WAN are likely to have the greatest impact:

- Main focus on supporting and optimizing applications in real time
- Focus on increasing security
- Enable business managers to achieve their strategic objectives

- Expected change in WAN cost reduction
- Give priority to important things
- High input and output capability in the network

CONCLUSION

The elastic nature of direct cloud connectivity makes it possible for businesses to flex and scale depending on immediate needs. Instead, businesses can order services as needed, scale them to meet user needs and turn them off without notice. These services are immediately available without having to wait to bring new foundations and applications up to speed. This extreme flexibility makes it easy to transfer large amounts of data and keep workflows portable. Businesses can ramp up bandwidth and services immediately when dealing with a spike in trafficwithout losing service or seeing websites crash. A high level of flexibility is a must when dealing with data backup or disaster recovery situations. To achieve priority, provide administrative and economic requirements meet challenges and deliver new services and applications, organizations needboth flexibleand secure applications as well asnew andhigh-performance designs for their users to focus on data center infrastructure to be responsive and secure as well as expanding bandwidth and increasing security.

REFERENCES

Ab Rahman, N.H., N.D.W. Cahyani and K.K.R. Choo, 2017. Cloud incident handling and forensic-by-design: Cloud storage as a case study. Concurrency Comput. Pract. Exp., Vol. 29,

Alam, Q., S.U. Malik, A. Akhunzada, K.K.R. Choo and S. Tabbasum *et al*., 2017. A Cross Tenant Access Control (CTAC) model for cloud computing: Formal specification and verification. IEEE. Trans. Inf. Forensics Secur., 12: 1259-1268.

Cai, D.L., P.H. Wang, Y.C. Wang, F.H. Tsai and J.S. Wang, 2015. The implementation of peer-to-peer bandwidth estimation mechanism in multimedia streaming networks. Soc. Sci., 10: 1574-1582.

Garrison, G., R.L. Wakefield and S. Kim, 2015. The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. Int. J. Inf. Manage., 35: 377-393.

Hamid, A.H. and M.M. Yusof, 2016. Conceptualizing global cloud landscape: A review of adoption issues and challenges. Res. J. Appl. Sci., 11: 333-339.

Hawramani, I., 2017. Cloud Computing for Complete Beginners: Building and Scaling High-Performance Web Servers on the Amazon Cloud. Independent Publisher, Chicago, Illinois, USA., ISBN:9781520633169, Pages: 95.

Kar, J. and M.R. Mishra, 2016. Mitigating threats and security metrics in cloud computing. J. Inf. Process. Syst., 12: 226-233.

Khan, S.S. and R.R. Tuteja, 2015. Security in cloud computing using cryptographic algorithms. Intl. J. Innovative Res. Comput. Commun. Eng., 3: 148-155.

Manzano, M., K. Bilal, E. Calle and S.U. Khan, 2013. On the connectivity of data center networks. IEEE. Commun. Lett., 17: 2172-2175.

Mink II, A.L., 2015. US Federal Agencies and cloud: A common decision framework for determining which legacy IT systems should migrate to cloud. Ph.D Thesis, George Mason University, Fairfax, Virginia.

Nelson, P., 2015. Cybercriminals moving into cloud big time. IDG Communications, Framingham, Massachusetts, USA. https://www.networkworld.com/article/2900125/malware-cybercrime/criminals-moving-into-cloud-big-time-says-report.html

Osanaiye, O., K.K.R. Choo and M. Dlodlo, 2016. Distributed Denial Of Service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl., 67: 147-165.

Qi, H., M. Shiraz, J.Y. Liu, A. Gani and Z.A. Rahman *et al*., 2014. Data center network architecture in cloud computing: Review, taxonomy and open research issues. J. Zhejiang Univ. Sci. C, 15: 776-793.

Singh, S., P.K. Sharma and J.H. Park, 2017. SH-SecNet: An enhanced secure network architecture for the diagnosis of security threats in a smart home. Sustainability, 9: 513-532.

Sivasankari, T. and S. Sivasankaran, 2015. A secure strategy using weighted active monitoring load balancing algorithm for maintaining privacy in multi-cloud environments. Intl. J. Sci. Technol. Eng., 1: 232-237.

Somani, G., M.S. Gaur, D. Sanghi, M. Conti and R. Buyya, 2017. DDoS attacks in cloud computing: Issues, taxonomy and future directions. Comput. Commun., 107: 30-48.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.