

Study of Challenges and Possibilities of Building and Efficient Infrastructure for Kurdistan Region of Iraq



Abdusalam Abdulla Shaltooki, Dana Faiq Abd, Zaid Ahmed Hamid, Zana Azeez Kakarash, Omed Hassan Ahmed

Department of Information Technology, University of Human Development, College of Science and Technology, Kurdistan Region, Iraq

ABSTRACT

Digital communications play fundamental role in routine life. Requests for e-services and e-applications obviously will grow rapidly on networks. Although in Kurdistan Region, there are many potential barriers such as availability network infrastructure, delay, and security matters. However, design and implementing national digital backbone infrastructure are a lively and challenging task for the regime to better public sector efficiency. For the use of this research to get a sensation, of which barriers are more probable than others, a study was carried among the Kurdistan information and communication technology professional. Moreover, one of the primary focuses of this survey is offering Kurdistan Region Government a comprehensive, safe network infrastructure plan with minimal latency, high availability, and maximum performance different scenario have been examined by the simulation to represent different implementation ways. In the end, the possibility of applying cloud computing inside the setting of normal government operations and public services, in general, has been hashed out.

Index Terms: Cloud Computing, Kurdistan Region Government, National Digital Backbone, Network Infrastructure, Public Sector, Secure Network

1. INTRODUCTION

Digital communications play a fundamental role in everyday life. Technologies such as smartphones and broadband are modernizing the way we purchase commodities and services; the way we socialize, work, and also the way we are kept current in world events. Request for e-services and e-applications obviously will grow rapidly on networks. Moreover, the importance of information and communication technology (ICT) system has extremely become crucial for

governments to reduce routines, improve transparency, avoid corruption, systemize governmental processes, easy internal communications, and enhance productivity. For these reasons, most developed countries are extremely relying on increasing IT projects to provide better services for their citizens and to enhance collaboration between their directories [1]. As an example, according to the UK Digital Strategy 2017, to make sure everyone in the UK has access to fast, reliable broadband, the government has set out a vision for a superfast broadband network in the UK of over 24 Megabits per second, to reach 95% of the population by 2017 [2]. Governments are responsible to ensuring that their country has the right digital communications infrastructure that is high capacity, reliable, robust, secure, affordable, and fast. In developing countries like Kurdistan Region of Iraq (Kurdistan Region Government [KRG]), significant efforts to expand the ICT infrastructure have been underway for

Access this article online

DOI: 10.21928/uhdjst.v2n2y2018.pp15-23 E-ISSN: 2521-4217
P-ISSN: 2521-4209

Copyright © 2018 Shaltooki, *et al.* This is an open access article distributed under the Creative Commons Attribution Non-Commercial No Derivatives License 4.0 (CC BY-NC-ND 4.0)

Corresponding author's e-mail: Abdusalam Abdulla Shaltooki, Department of Information Technology, College of Science and Technology, University of Human Development, KRG, Madhya Pradesh, India. E-mail: Salam.Abdulla@uhd.edu.iq

Received: 11-08-2018

Accepted: 17-08-2018

Published: 22-08-2018

several years, and we intend for ICT to be useful to all sectors of society such as education, health, the economy, and government [3,12].

However, the motivation of this paper current state of backbone network development in Kurdistan Region is in a disappointing situation. Many factors such as war, lack of transparency and plan, lack of ICT professional and consultancy in the power, ICT project failures, culture, lack of electricity, and many others are the main causes for the current situation.

The broadband commission for sustainable development is evaluated digitization in different countries across the globe on September 2016. According to their list of national broadband policies, a number of countries with National Broadband Plans are 151 while a number of countries, including KRG-Iraq, planning on introducing a national broadband plan are 7 and a number of countries without national broadband plans are 38 [4].

On April 2017, we sent an invitation through email to the IT professionals, asking them to complete an internet-based survey which was asking “in Kurdistan Region, what are the top potential barriers to implementing national digital backbone infrastructure?” According to our survey which has been shown in Bar Chart 1, 81.8% of respondents believe that poor government ICT strategies and action planning are the top barrier while 72.2% of them condemn political visionary leadership. Moreover, corruption has been mentioned as the main cause by 55.6% of respondents and underdeveloped governance structure by 50% of them. Almost 36.4% of them said poor choices of some of the ICT consultancies and education and culture issues. The 40% of others chose lack of skilled and unskilled labor force option, and 34% claim that below standard of performance by some of contracting companies. Finally, 33% replied that indifference and ignorance and selfishness of some of employees are the main cause. However, still, 39% selected lack of adequate international support and contribution choice.

KRG as a developing country needs to establish a network infrastructure design that will be able to support all the governmental directorates. The research offers a complete look at the network design that would be implemented at all KRG locations. It requires that a network solution offers minimum latency, high availability, and maximum performance. Also, best technology uses in this solution to meet KRG requirements. Details are also presented to the Kurdistan Region, and we are confident that will meet and exceed the expectation of Kurdistan Regional Government. To ensure that all design aspects are

properly conveyed to the Kurdistan Region, it includes several detailed diagrams of all locations (Sulaimany, Arbil, and Dhok) connecting with high-speed technology along with summaries of the types of technologies that will bring life to the network designs and also provide security management to protect sensitive network assets. Illustrated with diagrams will highlight the logical design and physical design.

Furthermore, since 2009, many governments started the process of replacing local computers with cloud platforms. Many developed countries such as the USA, the UK, Japan, South Korea, and Germany have already leveraged cloud computing in the public field and realized budget reductions and carbon emission reductions for green IT implementation. Therefore, our government should eventually seek new and innovative solutions for the future IT service environment, to realize high-efficiency green government IT [1].

The remainder of the paper is organized as follows: Section 2 provides background information and identifies used tools and technologies. In section 3, we will introduce the security issues. In section 4, literature review, and in section 5, proposed design has been described. 6 focuses on using cloud computing in the government. Finally, conclusions are drawn in section 7.

2. BACKGROUND

In this section, we provide a brief background information in section 2.1, reviews the relevant literature to explain the existing research in section 2.2, and the steps we have used to carry out this research in section 2.3.

2.1. Metro Ethernet

Metro Ethernet is a standardized service, defines clear services, and interfaces to allow vendor and service provider interoperability, scalability. It has five “9” availability through end-to-end service level protection against any failures in the underlying layers [2].

2.1.1. Quality of Service (QoS)

QoS is one of the most important network characteristics to classify internet traffic for internet services to reduce the effect of busy bandwidth. At QoS, internet traffic is classified as high, medium, and low, higher traffic can be send first, such as voice, which is sensitive to delay [3].

2.2. Multiprotocol Label Switching (MPLS)

MPLS is a way to interconnect geographically dispersed corporate sites over a private connection. This is accomplished



Bar Chart. 1. Barriers to implementing national digital backbone infrastructure.

through the deployment of MPLS/virtual private network (VPN) services such as MPLS IP-VPNs or virtual private local area networks (LAN) services. MPLS is a scalable, protocol-independent transport method. In which data packets are assigned a label, whose content determines how a packet is forwarded through the network without having to examine the packet itself.

In a regular IP network, when a data frame is received by a router, the router examines frame and pulls out the packet information and then checks

the destination IP address. If the destination address does not match any configured address on the receiving router, then a lookup is done in its routing table to determine if the packet is discarded or the direction in which to forward the data packet. Comparably, in an MPLS network, the forwarding of data traffic is done a bit differently. When a data frame is received by a router, it can either be labeled or unlabeled depending on if it was forwarded using a CEF or LFIB lookup [4], [5].

2.3. DMZ Screen Subnet

Often, it is not possible to block all traffics into your network. If you host a public website or email server, you need to allow inbound connection on a limited basis. The DMZ is a semi-private network that uses to host services that the public can access. Users have limited access from internet to systems in the DMZ to access these services [6].

2.4. Security Management

One of the significant sectors so that KRG can permanently provide the best service to the region is security management. Security management can monitor network traffic to detect malicious attack, discover a network vulnerability, and prevent network from spoofing. Security management can guarantee

to offer confidentiality to protect privacy, integrity that means the sender sends data and receiver gets the same data without change. KRG security management comprises a lot of tools and techniques those are encryption, physical security, perimeter security, stateful firewall, intrusion detection systems/intrusion prevention systems (IDS/IPS), security applications, access control, and VPN.

2.4.1. External and internal security

The critical missions of a KRG network are security. Hence, it should be establishing strong security countermeasures and the best approach to provide better security by deploying a multiple approaches against external and internal threats.

External security, the first point is policy, procedures, and awareness. Policy is a set of rules and principles which are written to govern all KRG areas to secure the assets.

The second point to protect network from internal threats. Implement network access control (NAC) to add more security before any device connects to your network. Use least privilege policy to get users most restrict accesses to data. In addition, installing personal firewall and IDS software on all hosts. Applying security patches to network devices to ensure against new threads. Least privilege - user or process is given access only for what is required to perform their job duties [7].

- Usernames
- User ID
- Account number
- Personal identification number
- Radiofrequency identification badges and smart cards

IPSec provides the following network security services.

- Data confidentiality - The IPSec sender can encrypt packets before transmitting them across a network.
- Data integrity - The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data have not been altered during transmission.
- Data origin authentication - The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent on the data integrity service.
- Antireplay - The IPSec receiver can detect and reject replayed packets. Cisco IPSec prevents routed traffic from being examined or tampered with while it travels across a network [8].

2.4.2. Encryption

Encryption is defined as a method for taking a message from plain text and transform into style so that unauthorized person cannot understand which is called a cipher form.

Encryption is a key point to KRG which is required to encrypt every data before send it through the internet because without encryption KRG cannot gain data confidentiality. Encryption provided by a high-performance algorithm such as triple data encryption standard and advanced encryption standard [8].

2.4.3. Physical security

Physical security is a method to protect KRG resource from physical attacks such as intrude data center, building, account, and IT building. . . . KRG needs physical security implementations so that to prevent any violations and threats that damage network assets. There are a lot of counter measurements that require to implement and to protect physical resource of KRG network. The following physical designs deploy to prevent expected interception and intrude KRG assets [9].

2.4.4. Firewall

Firewall is a security system or device to prohibited unauthorized users to access private network. Firewall applies policy, which is based on rules to filter and inspect all traffics traversing across network. In addition, firewall can be hardware or software or comprises both of them [10].

2.4.5. Intrusion detection/prevention systems

IDS/IPS: KRG network needs additional layer security, which is considered the best security solution that is IDS/IPS.

IDS/IPS is a process to analyze and monitor network inbound and outbound traffics to assure the sanity of KRG network [11].

2.4.6. VPN

A VPN is an encrypted connection between private networks over a public network such as the internet. VPN uses virtual connections called VPN tunnels instead of a dedicated layer 2 connection such as a leased line. VPN tunnels are routed through the internet from the private network of the organization to the remote site or employee host. VPNs provide sufficient level of information security using advanced encryption and authentication protocols which protect data from unauthorized access.

3. LITERATURE REVIEW

Many researchers have recently focused on the digital network infrastructure as a main challenge for developing countries. Al-hashimi *et al.* and Haider *et al.* mentioned in [14], [15] one of the main problems in Iraq is lack of network infrastructure. Furthermore, Bahar *et al.* described useful information on the challenges and current status of

the backbone infrastructure and internet in the KRG which provided by private companies from several countries, namely Iraq, Iran, Turkey, and the others such as Azerbaijan [17,18]. The focus of [16] is to investigate the main challenges and obstacles facing e-services provision including lack of well-established network infrastructure and proposes a design solution that will help KRG to overcome some of these challenges [5]. It aims to identify primarily causes of several IT project's failures including national backbone with KRG and comparative with several other IT projects success and failure within developed countries such as Turkey, UAE, and Estonia. The objective of Adulsalam *et al.* [3] is the enhancement of good governance by the deployment of a modern and secure e-government broadband infrastructure. Aziz's *et al.* paper introduces the design of telemedicine project and discusses the possibility of implementation for different system according to the available technologies and needs. In the Al-Samarrie's *et al.* work, the design, analysis, and evaluation of an optimum WiMAX proposed network are performed according to this E-government project requirements in the city of Baghdad [13]. S. Shenker *et al.* proposed to set up a virtual health centers include websites, public health centers, medical clinics, and linking them with instruments and smartphones by providing information of physicians and medical services provided and citizen media deadlines as well as linked to social networking sites [20]. Seifedine and Hassan [19] mentioned the importance of using security such as IPSec and VPN to establish secure connection through shared networks. Specifically, the project should enhance coordination of public service delivery across ministries, key agencies, and local governments. It will also strengthen existing government data centers and portals and improve access to e-services for state building such as automated administrative services including e-payroll, civil registration, e-health, e-procurement, e-customs, and revenue management.

4. DESIGN AND ANALYSIS

4.1. Design Description

The Kurdistan Region in Iraq is a very wide area in the north of Iraq and can be divided into three main states, i.e., Dhok, Erbil, and Sulaymaniyah for connecting the main infrastructure equipment as illustrated in Fig. 1. Every location in KRGs states network required special attention because each location had different mission-critical as well as government priority needs that service needed to meet. The Dhok, Sulaymaniyah, and Arbil locations needed to have several high-speed links, with availability that guaranteed

99.99% or close to it redundancy and excellent network performance. In addition, Kurdistan Region, requirements centered on security, reliability, availability, and performance. Hence, in our design, we have made it equally in all requirements for the whole region.

Fig. 1 can show that all the connections have been done with backup connections with high data rate performance type like the design represent that each region has been provided an internet connection with two different ISPs for more reliability. Moreover, suitable Telecommunication Companies are proposed that could deliver all the services required to meet the KRG goals. The infrastructure network design focused on high availability and reliability using dual ISP as redundancy. TeliaSonera Telecommunications and Cogent Company could select as the two ISPs that could offer the best service levels and technologies to meet KRGs wide area network (WAN) requirements. Furthermore, providing much higher performance and low latency through single-mode fiber optic cables directly connects to all cities. The technology that we have selected to interconnect all of the KRGs core sites is MPLS, MPLS switching for high performance, low latency, and high availability issues as well using dual ISP as redundancy. The design also provides the

network from single point of failure and provides scalability since it can be easily added more service and devices. Another point, availability that is guaranteed 99.99–99.999% or close to it. Finally, for each city, there are two powerful routers, which provide network from a single point of failure, if one of them does not work, the other one can take place another one.

4.2. Logical Diagram

The logical diagram in Fig. 2 illustrates the design that could be selected to implement at the Sulaimani location. It shows the redundancy strategy that we used for all network equipment and WAN links that connect to TeliaSonera ISP and Cogent ISP. Virtual VLANs for the Sulaimani locations are also depicted to show departmental segmentation at the location. Finally, security devices are shown to illustrate how the locations information will be secured. All locations are identified by name while the connection types are color coded and labeled in a legend within in the diagram.

The design uses dual ISP for both internet and MPLS as redundancy to provide low latency and high availability. There are two powerful routers which are directly connected to the server providers to bring services to the Sulaimani network. Furthermore, behind the router, some firewalls used for

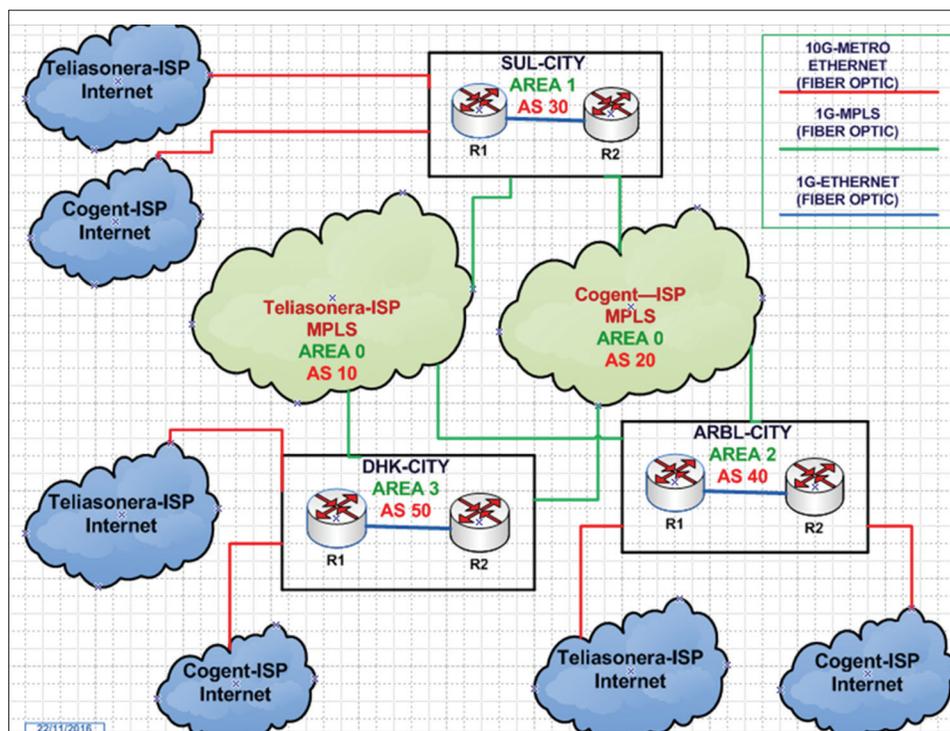


Fig. 1. Kurdistan Region Government infrastructure design.

security purpose since this is a very critical area and all the traffic come through. Furthermore, fiber optic cable uses for connection which provides higher performance and lower latency.

The design in Fig. 2 also shows the logical layout in the details of KRG Sulimaniyah location. VLANs are represented in this diagram to show how the different departments segmented in the network. The figure also shows the equipment, link types, and redundancy practices that are to be used for the location.

4.3. Internet Connectivity

To meet KRG internet requirements and to be sure no physical disconnect effect over the network connection, two internet service providers have been provided in the design to ensure the availability of internet services in the event of a disaster. We felt that this design aspect was crucial purely because of the financial nature of KRG business, where network outages would result in lost revenue. The ISPs that we selected to handle KRG WAN network were Cogent Telecommunications and TeliaSonera Telecommunications as mentioned before in the logical design.

These two providers were selected because they offered a wide variety of network services and link speeds that matched

well. With our intended network design, and because both ISPs had service level agreements (SLAs), that guaranteed 99.99% uptime for our internet services. The following are brief descriptions of the internet connections that were implemented at all KRG locations.

At KRG Sulaimani, each router was given a link to both Cogent and TeliaSonera ISP. The total links to the internet were 4, each of which was a 10 Gbps Metro Ethernet link.

This setup ensured excellent link redundancy and fault tolerance in case of a network failure. KRG core business being conducted at these locations.

4.4. Redundancy and Availability

The network infrastructure design for this location was set up to offer redundancy, security, and availability using dual ISP, redundant devices, and redundant links. In addition, metro Ethernet and MPLS technology can provide 99.99% and 99.999% availability, and redundant devices fiber optic links provide more availability.

Finally, SLA (service level agreements) automatically monitoring to keep the connection between ISP and KRG and can guarantee to afford best reachability and includes

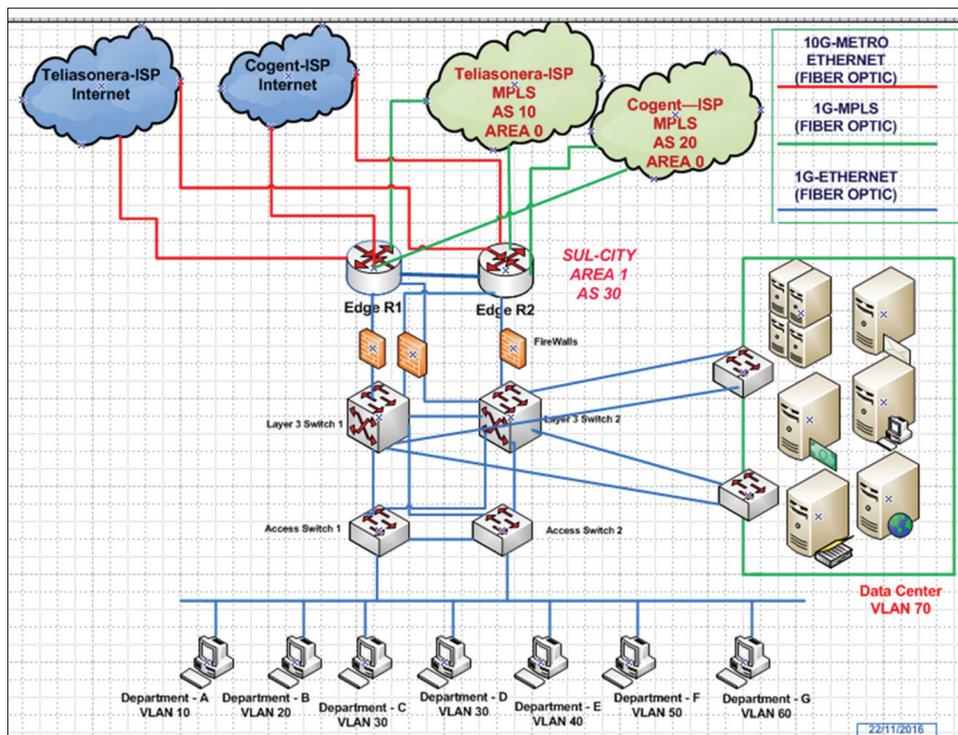


Fig. 2. Display logical diagram for the Sulaymaniyah city network infrastructure.

guaranteed level of network availability, network performance in terms of round-trip time, and network response in terms of latency, jitter, and packet loss.

4.5. Physical Diagram

The physical diagram shown in Fig. 3 that gives greater details on how KRG-Sulaimani location would be designed physically. The diagram highlights the redundancy implemented in the network so that maximum uptime is maintained. The security infrastructure is also shown in this diagram to give management an understanding of where security is needed. The security devices include firewalls, IDS, and IPS devices. At the data center, we implemented redundant links and installed two load balancers to that network resource request could be handled properly without delay or issue. First, IPS devices installed between ISP and Sulaimani core routers to protect the network from very critical malicious attack. Then, two core routers which are connected to the server providers to bring services to the Sulaimani network as illustrated in Fig. 3.

As a next layer security, some firewalls used to provide more security to the network which they are laid between core routers and layer three switches. Finally, to add another layer of security, IDS used to monitor all traffics come or out from the network.

5. EVALUATION AND DISCUSSION

Using MPLS over the old technology like ATM give a high quality of work in different aspects such as integration, greater reliability, low cost, scalability, and traffic routing. The traffic routing is the one we are looking for because MPLS works by imposing labels on packets as they allow a customer’s network and enter the MPLS network. Rather than look up IP header data to direct packets, network elements simply read the MPLS label and whisk the packet on to the next hop in a predefined route.

Other benefits of MPLS include greater reliability and predictability of traffic inside the network and packets only go along the routes they have been conducted on the configuration. This is a marked difference from IP routing, where one packet’s path could be distinctly different from the following based on network conditions at the time. Furthermore, the most important is the design scalability it’s one of the benefits of MPLS is that it combines some of the qualities of physical “nailed up” circuits that were difficult and expensive to scale, with the cost-effective but relatively unpredictable nature of pure IP routing, according to Errol Binda, senior marketing director of Aviat Networks.

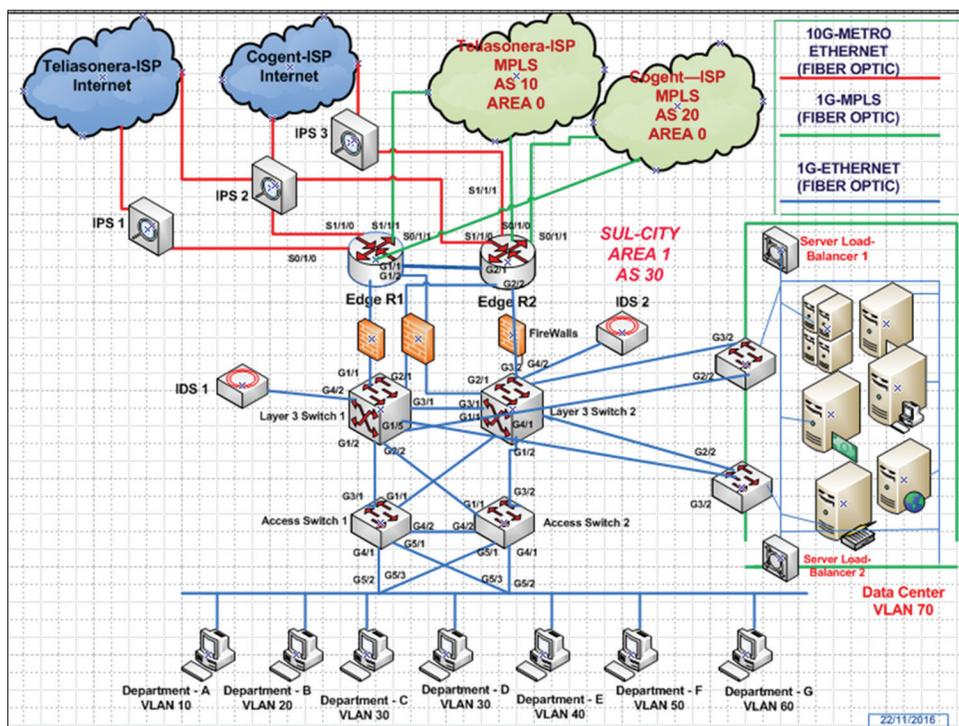


Fig. 3. Display the physical diagram for the Sulimaniyah city network infrastructure.

When it comes to the scalability of larger or more complex networks, if you have MPLS that allows you to do automatic configuration of the network and setting up of tunnels or label-switched paths. It is less resource-intensive physically to configure the circuits.

In summation, many different types of traffic can be carried through MPLS routing without regard to what type of traffic it is.

On the other hand, using a new WAN technology like the Software-defined- WAN (SD-WAN) that makes it potential to bond multiple WAN links, especially interim of unified Security protocols for provide the network end-to-end encryption across the entire network. Every location will have the same security configuration. As well as, SD-WAN will allow me to change my bandwidth and CoS settings in an instant, but this technology is still in the revision version. Hence, MPLS effectively makes the best utilization of bandwidth and security right now.

Furthermore, it needs virtually no control in the thing that will be in the cloud. Significantly, SD-WAN vendors might advise you with keeping an MPLS connection. Previously, parallel of the broadband connection to guarantees QoS to the ongoing movement in voice and video, there are some drawbacks to implement network infrastructure all of them were mentioned in details in introduction section.

6. USING CLOUD COMPUTING WITHIN THE CONTEXT OF NORMAL GOVERNMENT OPERATIONS

Cloud computers are superior to locally run data centers for a variety of reasons including cost, energy efficiency, availability, agility, security, and reliability [17].

More recently, the National Institute of Standards and Technology distributed a meaning from claiming cloud registering as takes after: “Cloud registering may be a model for empowering ubiquitous, convenient, and on-demand system get on an imparted pool about configurable registering assets (e.g., networks, servers, storage, applications, and what’s more services) that might be provisioned. Moreover, Cloud registering may be fast granted access and use less management effort or less administration supplier cooperation” [4, 5].

The most important reason for introducing cloud computing to the public field is the reduction of at-large IT-related costs, which can serve as the best method to respond

actively to a dynamically changing environment. Careful analysis of the investment benefits and opportunity costs is certainly necessary before transitioning from the existing legacy environment to cloud computing. In particular, the introduction of cloud computing to public agencies requires intensive analysis and preparation based on public interest and security.

Once the validity of introducing cloud computing technology has been established, systemized plan such as EA should be chosen and promoted (Fig. 4).

Layers of cloud are infrastructure as a service (IaaS) that is developed on the virtualization technology, platform as a service (PaaS) that makes applications within the programing language, and software as a service (SaaS) applications that to be installed responsible by this layer. Cloud layers are distributed on Sulaimany, Arbil and Dhok cities for further network redundancy and service availability.

Every year in cloud computing, the number of participants and enterprises growth rapidly to get services from cloud service provider. Amazon Web Services (AWS) and Google are two supreme multiservice cloud services, and they can provide variety of networking services to their customers such as SaaS, IaaS, and PaaS. Hence, KRG can make an SLAs with AWS and Google cloud to get a variety of services, for instance, cloud computing software and application on a SaaS basis, cloud computing platform on a PaaS basis and running server, storage application, networking nodes, and other hardware on an IaaS basis. Although, these service providers can deliver better security and maintenance for KRG via SLA contract agreement.

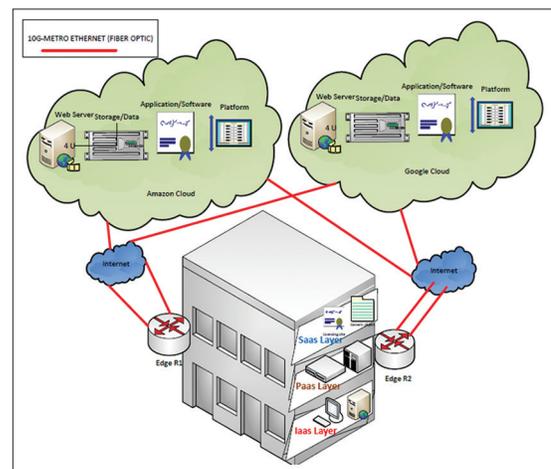


Fig. 4. Kurdistan Region Government Infrastructure Sulaimani HQ using cloud computing.

7. CONCLUSION

Digital communications play fundamental role in everyday life. The current state of backbone network development in Kurdistan Region is in a disappointing situation. These states are motivated according to our survey there are many potential barriers to implementing national digital backbone. The research offers a complete look at the secure network design that would be implemented at all KRG locations. Additionally, apply powerful network technologies such as MPLS and Metro Ethernet to meet KRG system requirements. Furthermore, the physical connection like fiber optic and 10 Giga Ethernet represented by topology type has a big effect to get the minimum latency $<0.3 \mu\text{s}$, high availability which is 99.99%, and maximum performance characteristics of the designed solution have been evaluated and discussed. Finally, using cloud computing within the context of normal government operations has been proposed for budget reductions and carbon emission reductions for green IT implementation. As well as, the cloud computing shows that can function as the best method to react actively to a dynamically changing environment through the network infrastructure.

REFERENCES

- [1] B. M. Amen, R. M. Nabi and S. M. Mahmood. Article: An investigation in IT projects failure within Kurdistan regional government of Iraq. *International Journal of Computer Applications*, vol. 133, no. 2, pp. 33-39, 2016.
- [2] K. Bradley. UK Digital Strategy 2017. GOV.UK. Available: <https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy>. [Last Access Details: 2018 Jan 21].
- [3] A. Adulsalam, A. Abubakr, M. I. Ghareb and H. Mahmud. "E-Payment: Prospects, challenges and solutions in KRG public sector." *International Journal of Engineering And Computer Science*, vol. 4, no. 9, p. 14092, 2015.
- [4] C. Sue. Accountability Arrangements to Combat Corruption-Synthesis Report and Case Study Survey Reports. © WEDC, Loughborough University, 2007.
- [5] D. C. Casimer, editor. Handbook of Fiber Optic data Communication: A Practical Guide to Optical Networking. Academic Press, New York, 2013.
- [6] B. Keith and S. Morris. CCNA Security 640-554 Official Cert Guide. Pearson Education, Förlag, 2012.
- [7] N. Stephen and J. Novak. Network Intrusion Detection. Sams Publishing Indianapolis, IN, 2002.
- [8] R. P. Thomas. Information Security Fundamentals. CRC Press, London New York Washington, D.C, 2013.
- [9] A. Noura. "A Comparison of the 3DES and AES Encryption Standards." *International Journal of Security and its Applications*, 9(7), 241-246.
- [10] K. McCasland. "Mastering Network Design with MPLS." Windstream Whitepaper, 2015.
- [11] J. Bleiberg and M. Darrell. Analyzing the Federal Government's Use of the Cloud West Monday, February 9, 2015.
- [12] L. Hyeong-Ok and M. Kim. "Implementing cloud computing in the current IT environments of Korean government agencies." *International Journal of Software Engineering and its Applications*, vol. 7, no. 1, pp. 149-160, 2013.
- [13] J. S. Aziz, O. A. Hussein and A. Naoom. "Design of telemedicine systems for rural and urban areas in Iraq." *ARPJ Journal of Engineering and Applied Sciences*, vol. 4, no. 2, Apr. 2009.
- [14] A. K. Al-Samarrie, H. Alyasiri, A. H. Al-nakkash. Design and analysis of wimax e-government network for the city of Baghdad. *International Journal of Scientific and Engineering Research*, vol.6, no. 1, Jan. 2015.
- [15] Cisco Networking Academy. Connecting Networks Companion Guide. Pearson Education, India, 2014.
- [16] H. Lee, M. Kim. "Implementing cloud computing in the current IT environments of korean government agencies". *Int J Software Eng Appl*, vol. 7, no. 1, 2013.
- [17] M. Al-hashimi, S. Mohanaad, H. Maytham and E. Abdalla. "Address the challenges of implementing electronic document system in Iraq e-government-Tikrit city as a case study." *Journal of Theoretical and Applied Information Technology*, vol. 95, no.15, pp. 3672-3683, 2017.
- [18] A. Haider, M. Bahari, H. Hashim, A. Bakri and W. Ismail. "Prioritizing implementation factors of electronic document management system (edms) using topsis method: A case study in Iraqi government organizations." *Journal of Theoretical and Applied Information Technology*, vol. 88, no. 2, pp. 375, 2016.
- [19] K. Seifedine and W. Hassan. "Design and implementation of system and network security for an enterprise with worldwide branches." *Journal of Applied Sciences Research*, vol. 4, pp. 1361-1370, 2005.
- [20] S. Shenker. "Fundamental design issues for the future Internet." *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 1176-1188.