Design concepts of a high performance enterprise campus network with high availability to support enormous traffic (Data, Voice and Video)

[1]Sanjith S L

[1]ICT Department,

[1]Indian Institute of Management Tiruchirappalli, Tamilnadu, India

Abstract : Campus network of an enterprise is a building or group of buildings that are connected to one enterprise network infrastructure that consists of many local-area networks (LANs). The enormous usage levels of online intranet and internet applications have hit the roof due to the litheness of these applications and platforms. The ever growing online platforms with it's ease of use aspects have made all organizations and individuals turning to online-based solutions. The drastic growth of IoT applications have also made a tremendous increase in the utilization of network bandwidth. The design of a network considering the foreseen growth has become a challenge due to the limitations of that are still persists on the network components/devises. In this paper we are discussing about the designing and implementation of an enterprise campus network infrastructure which has been developed and implemented in an enterprise campus during it's testing phase which can support upto 100 G backbone considering all the requirements of a fully automated smart campus setup. This design also has a Disaster Recovery centre which works on active-active mode for real-time redundancy through which the effective bandwidth could be boosted upto 200 Gbps through link aggregation. The design process has been gone through different progressions and ensembles which has finally come up with a state of the art campus infrastructure which could run all the IT related requirements of the campus seamlessly atleast for 10 years down the line without any major change in the passive and active of the backbone infrastructure.

IndexTerms – **Enterprise campus network, High- speed network , Network redundancy , active-active network, 100G ready network.**

I. INTRODUCTION

Applications have become a key driver of revenue, rather than their previous role as merely a tool to support the business process. What acts as the heart for all applications is the network providing the connection points. The conventional methods of network implementations are facing challenges in managing the huge data traffic that are happening in the network due to the drastic increase in the number of devices and heavy load in terms of usage. Due to the new, critical importance of the application layer, IT professionals are looking for ways to improve the architecture of their network. A network that consists of only 50 meshed routing nodes can pose complex problems, which may lead to unpredictable results. Attempting to optimize networks that feature thousands of nodes can pose problems that are even more complex. The devices that are connected with the network are different in nature and we are in a scenario at which anything and everything could be connected to the network to fetch/transfer the data. This has created necessity of huge requirement of bandwidth for the seamless and effective functioning of the network applications. There are passive technologies like Optial LAN, CAT 6 A etc which has contributed for building a passive infrastructure more effective, stable and robust. The technologies like FTTH has also provided solutions for making high bandwidth network to overcome the drawbacks in the conventional copper local area network. However, most of the medium and small sized enterprise organizations have not started adopting these technologies due to the substantial cost that required in the implementation of these technologies. But the technologies have to be identified and designed as per the physical scenario and requirement without which the performance can not be improved.

Capacity planning, distance between the buildings, routing of conduits and cables, identification of passive technology, identification of data centre and disaster recovery centre, locating/positioning of hub-rooms, positioning of access racks etc are the major points to be considered in the construction of the passive infrastructure. The configuration parameters, zone wise user requirement, VLAN design, security aspects, content filtering policies for each zone, intrusion detection functionalities etc are the key points to be considered while designing the active infrastructure of an enterprise campus. The applications like WiFi, VOIP, Video Conferencing platforms, IP based surveillance system, automated audio visual requirements, in-house server applications etc also needs to be considered while designing an active infrastructure of an enterprise campus network.

A strategic identification of suitable topologies and architectures are essential in the designing of a campus network for getting better performance and reliability. Depending on the nature of users and applications, the architecture has to be designed in each zone of the campus. The economic approach with effective utilization should also be a criteria in the designing of a campus network. This work focused on designing a complete network of a campus which consists of townships with villas and apartments, clinic, Lodging/hostels, classrooms, offices, library, computer centre etc. The similar strategy can be applied in any campus environment (academic/industry/township) for the proper implementation of it's network infrastructure.

II. PREREQUISITES

The prerequisites that are required for setting up the IT Infrastructure have been evaluated and made necessary steps for making the prerequisites ready during the construction of the buildings. The major prerequisites that have been considered are detailed below.

2.1Architecture:

First of all, the topology be followed for the development of the passive backbone infrastructure has been finalysed without which it would be hard to realize the prerequisites that have to be arranged. The network architecture is another important factor that needs to be finalized before the beginning of the task. The roadmap created for these prerequisites are explained below:

a) Backbone Topology:

Finalization of topology is an important factor for the kickoff of the installation of the Network Infrastructure. It had been freezed to go in for a combination of star and ring topologies for the backbone network and the details are shown in figure.1 below.
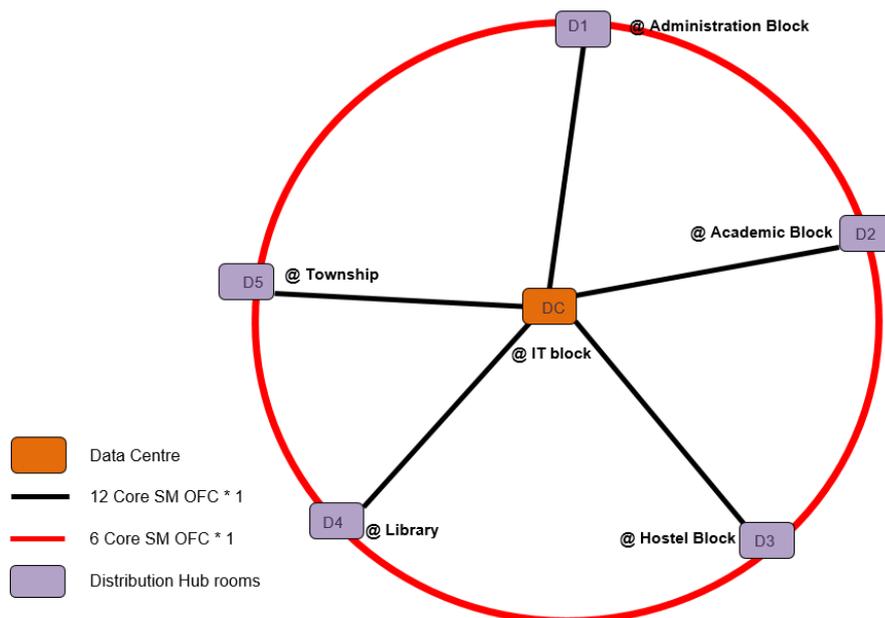

Figure.1 : Combination of star and ring topologies for the backbone of the enterprise campus network

In addition to the above, star connectivity has also been made from the disaster recovery centre for redundancy for which 6 core optical fiber cables have been laid between the DR centre and each distribution hub rooms. The disaster recovery centre has been made in a building which in a building that is far away from the data centre.

b) Architecture:

It was planned to implement a 3 tier architecture (Network with Core, Distribution and Access) with Core distribution and access based on the geographic locations. Feasibility study has been made on the possibility of 2 tier architecture and noticed that the high end switches have to be installed in all the distribution hub rooms which may cause significant increase in the budget. Accordingly, cabling layouts have been made, trenches have been constructed (wherever required), pipes have been laid and the concealed conduits were also fixed during the civil construction phase itself.

2.2Capacity Planning and location of Distribution Hub rooms:

Capacity planning has been done for each building. Based on the number of ports that are required in each building, its geographical locations and the nature of users in these buildings, five different zones have been created. A suitable area has been identified almost at the centre of each zone. Following this method, five distribution hub rooms have been located and the locations are given below:

1. First distribution hub room (D1) with 10' X 10' dimension has been located at the Administration building for connecting all the access racks installed in that block.
2. Second distribution hub room (D2) has been positioned at the ground floor of the Main campus building for connecting all the access racks installed in that block.
3. Third distribution hub room (D3) has been placed at the ground floor of a building located almost at the middle of the hostel buildings for connecting the access racks installed in each of the hostel building via outdoor OFC.
4. Fourth distribution hub room (D4) has been positioned at a room which is located at the middle of the housing zone (township) for connecting the access racks installed in the villas, apartments, guest houses, commercial complexes etc.

5. Fifth distribution hub room (D4) has been sited at a room which is located in a four storied building for connecting the access racks installed in the computer centre, labs, library etc.
6. There can be n number of distribution hubrooms depending on the geographical structure and load

The OFC connectivity diagram between the access racks and D1 has been made as given in figure.2 .

III. PASSIVE INFRASTRUCTURE

Pros and cons of all the prevailing architectures and methods that are available for the passive infrastructures have been analyzed and then identified a suitable models for each component of the passive infrastructure. A study has been made on the available passive physical connectivity options (cables) and it's performance in terms of distance and speed and the points noted are given below:

Table 1: Types of cable and it's performance/distance limitations

Sl. No	Cable Type	Distance limit (upto)
1	Coaxial Cable	500 Meters
2	Copper, CAT6 A – CATx	100 Meters
3	Copper, CAT6/ CAT 5e – CATx	100 Meters
4	Multi Mode Fiber – Optical fiber cable	550 Meters
5	Singe mode fiber	20 Kilo meters

Apart from the conventional system, the possibility of FTTH / Optical LAN has also been perused. There was huge increase in the cost for Optical LAN compared to the conventional method. After a detailed study on the available copper Ethernet twisted pair cables, it has been decided that CAT 6 A would be ideal for the copper connectivity that provides 10 Gbps bandwidth which could be connected to the Ethernet switch without any media converter and suitable for future scalability of the network. Hence copper cables have been used for the connectivity between the end device (computers, access points, cameras, telephones etc) and access racks. Accordingly, the access racks have been positioned such a way that the distance between the user and the rack does not exceed 90 meters.

Optical fiber cables have been used for the core - distribution and distribution – access connectivity. Armored outdoor cables have been used for the exterior applications and indoor cables have been used for the indoor cabling. Considering the distance and performance, single mode optical fiber cables have been used for all the optical fiber connectivity between the access and core which can provide upto 20 kilometer distance without any amplification. 12 core outdoor armored cables have been used for connecting the core switch with the distribution switches in star topology and 6 core cables have been used for the ring backbone connectivity. While providing connectivity to the villas, street cabinets have been used. 24 core cables have been laid from the distribution rack to the street cabinet. These cables have been spliced and terminated inside the street cabinet and extended the connectivity from these cabinets to the houses using 6 core OFC cables.
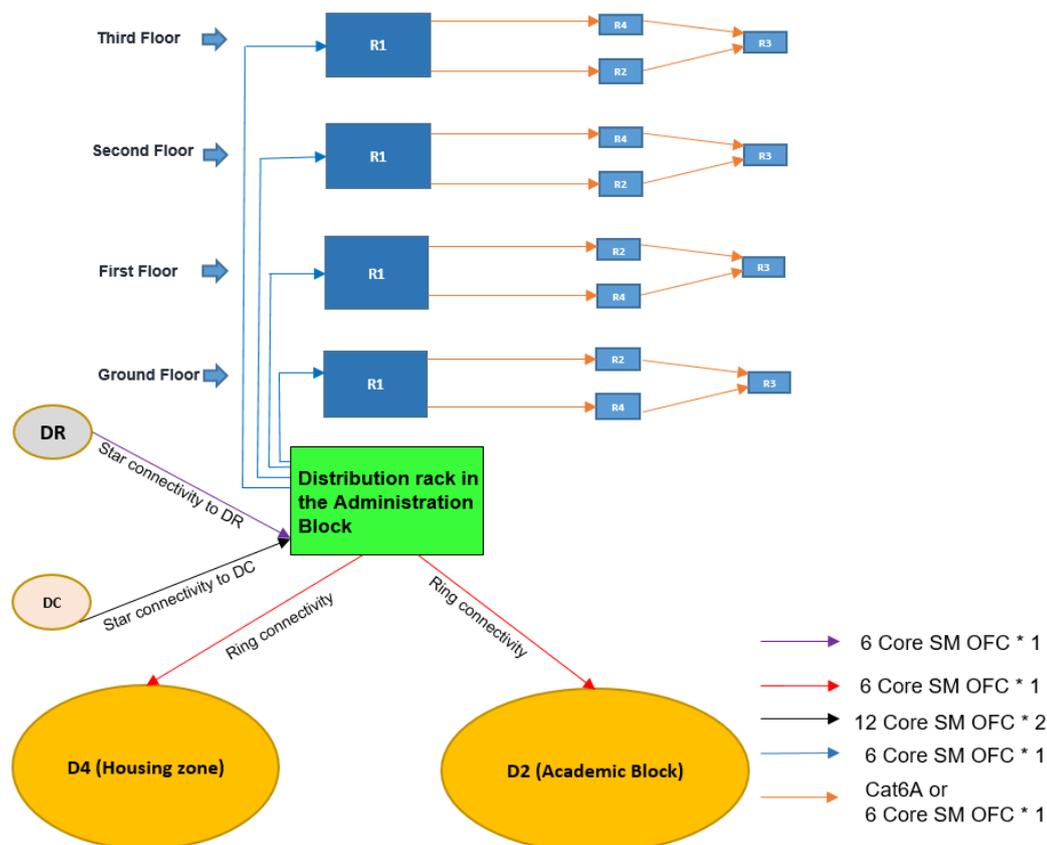
Figure 2: OFC connectivity diagram from D1 to the access racks of that building

From all the distribution hubrooms, ring connections have been laid to the adjacent distribution hub rooms using 6 core OFC cables. All the distribution hubrooms have been connected with data centre using 12 core OFC cable and DR centre using a 6 core OFC cables. Similarly physical cables have been laid from the core till the end user for establishing the network connectivity. This has provided three times redundancy between the core and distribution and two times redundancy between the distribution and access. All the access racks were interconnected in ring architecture such a way that there would be two OFC cables terminated in each access rack. The passive connectivity diagram of between D1 and the access rackes located in that building is shown in figure 2.

IV. ACTIVE INFRASTRUCTURE

Active infrastructure plays the major role in terms of performance of the network infrastructure. The active infrastructure should provide performance scalability and expandability. The availability of ports should also be available for the enlargement of the network as per the future requirement. It is the responsibility of the designer to oversee all the requirements that may arise in the future (at least 10 years down the line). The following parameters have been considered while designing the active infrastructure.

- Designed on III Tier Architecture with Core, Distribution and Access.
- Designed on a combination of Star and Ring topology for providing 99.9% uptime.
- Designed on Active – Active technology through which high availability has been ensured from core to access.
- Designed to work on Low Latency by reducing the HOP count.
- Designed to Work on Longer distance using Single Mode Fiber optic cables.
- Designed to work Harsh Environment condition by using industrial grade switches for outdoor application, which support high temperature and rugged environment.
- Designed for future technology with 100G ready network, which provides investment protection.
- Designed on Open Standards based Network Architecture.

The detailed schematic of the network infrastructure is given in figure 3 which shows the virtual connectivity diagram of all the major active components that are used for setting up a secured and stable network infrastructure
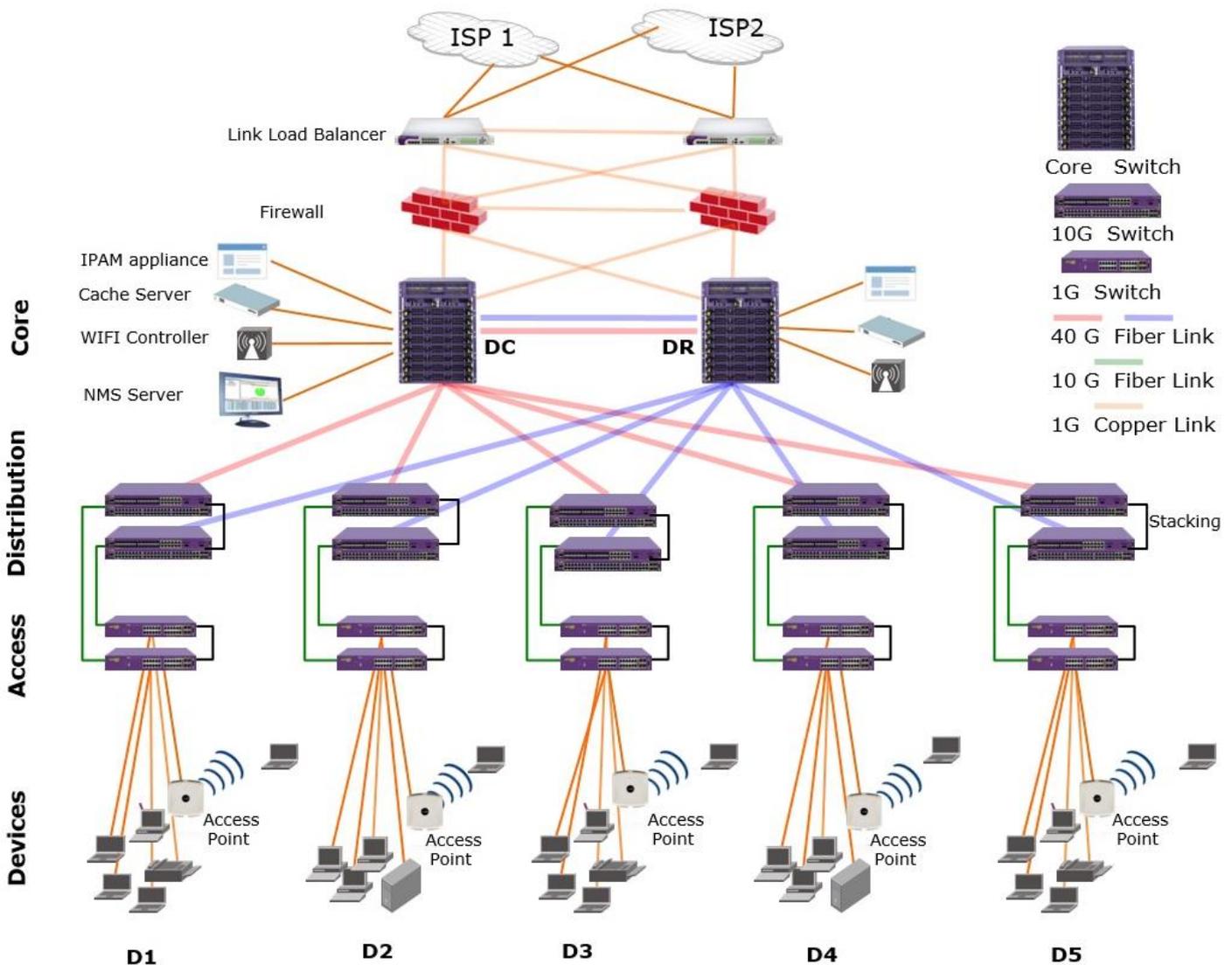
Figure.3 : Network schematic diagram of the active infrastructure of the enterprise campus network

4.1 Security and Load Balancing components:

A link load balancer (LLB) has been used for balancing the bandwidth utilization depending on the availability of bandwidth with each ISP and the and the bandwidth requirement of the users. LLB appliance is located between the ISP gateway and firewall distributes in-bound and out-bound traffic to and from multiple Internet Service Provider (ISP) links. Policies have been set using the Traffic management algorithms of LLB which ensure that all leased ISP links are being used to their best gain. Firewall has been installed as shown in figure 3 to monitor and control the incoming and outgoing network traffic based on predetermined security rules. The appliance that has been used as firewall also acts as an UTM box as this appliance has multiple security functionalities at a single point on the network which includes anti-virus, anti-spam, content filtering, web filtering etc. All these functions were enabled and content/web filtering policies were created as per the user requirement, which would protect the network from threats and attacks.

4.2 Network Switches:

A high capacity switch has been installed as core switch which has sufficient number of ports that supports upto 100 G bandwidth and the remaining ports supports 10 G. The core switch used for this setup is a chassis based switch which gives flexibility of scaling the ports as per the requirement by inserting line cards. The 100 G ports of the core switch are connected with the 100 G port of the distribution switches installed in the distribution hub rooms to achieve a bandwidth of 100 Gbps between the core and distribution. As shown in figure 3, there are two cables that are reaching the distribution hub rooms on which first cable is from DC (Data Centre) and the second cable is from DR (Disaster Recovery Centre). Each cable can provide 100 Gbps and together we get 200 Gbps bandwidth at the receiving end (Distribution hub room) through link aggregation. This also provides redundancy upto the distribution end. These cables are terminated on two different distribution switches and there are interconnection between all the distribution switches using stacking cables. After enabling stacking functionality on all the distribution switches installed in one distribution hub room, all these switches were acting virtually as a single switch.

The 10 Gbps ports of the distribution switches have been connected with the 10 Gbps ports of the access switches. First connection was coming from the first distribution switch which has been connected with the first access switch of the access rack. The second connectivity has been made from the second switch of the distribution rack to the last switch of the access rack. Then stacking has been enabled for the access switches after interconnecting the switches using stacking cable. The effective bandwidth for data

transmission would be 20 Gbps through link aggregation. Similarly configuration and connectivity have been made in all the remaining distribution and access racks. The virtual connectivity diagram representing the connections between the distribution rack and access racks is given in Figure 4
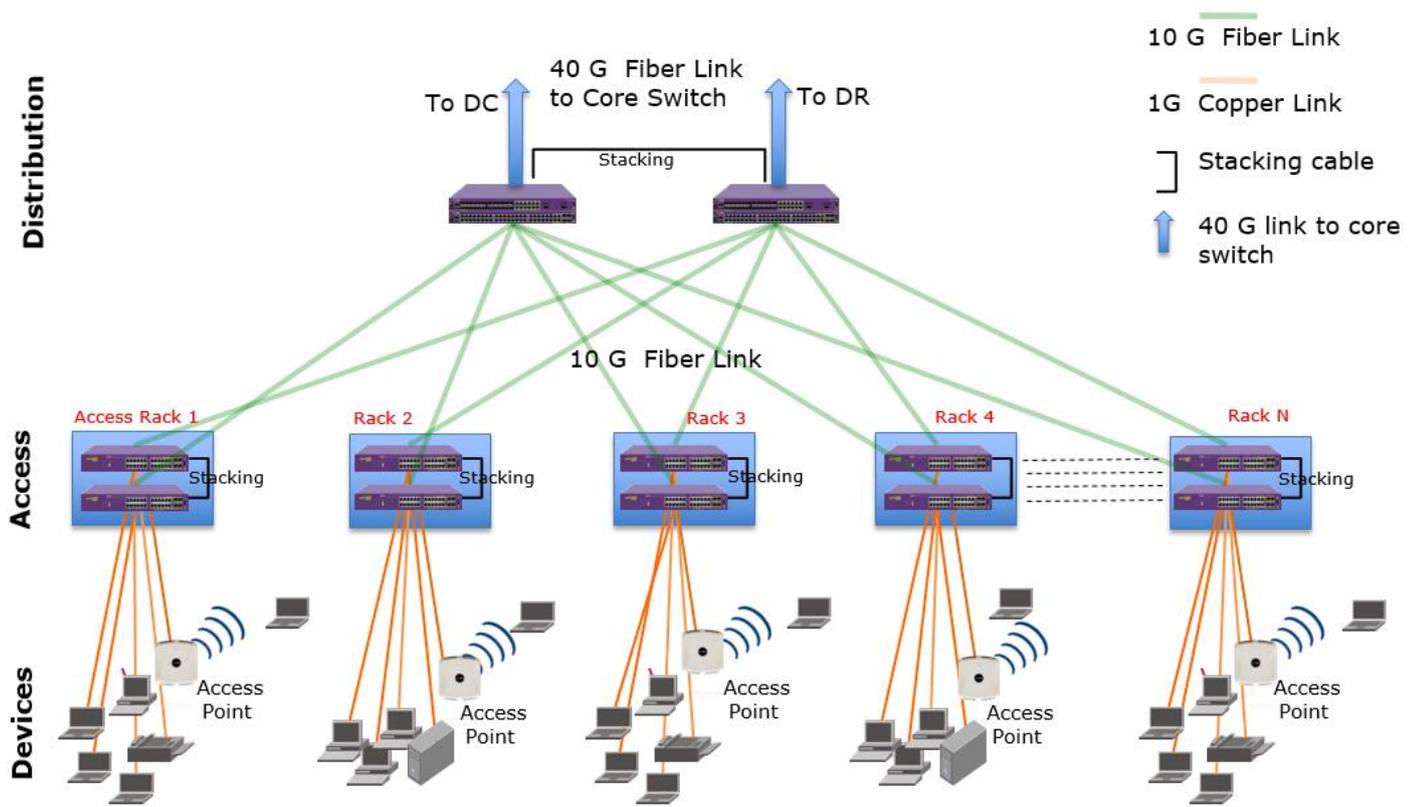

Figure 4: Schematic of the connectivity between Distribution and access racks

4.3 Management and monitoring components:

Network management System (NMS) software has been setup for the realtime monitoring and management of the complete network infrastructure. An IPAM appliance has been used for the dynamic IP address allocation (v4 & v6) and DNS. IP_ MAC binding has also been enabled for the required users. A cache server can also be setup to avoid the wastage of bandwidth while accessing the same content/data repeatedly.

4.4 Failover and High Availability:

Failover has been configured for the ISPs as well as all the major core components of this network which ensures 99.9 % uptime. The failover of the ISPs was also configured in the link load balancer such a way that ISP2 will handle the complete load when ISP1 is down and vice versa. All the core components are working on active - active mode which provides more efficiency and better performance. For enabling the active – active functionality and high availability, criss cross connections via OFC cables have been made between the components installed in DC and DR as shown in figure 4.
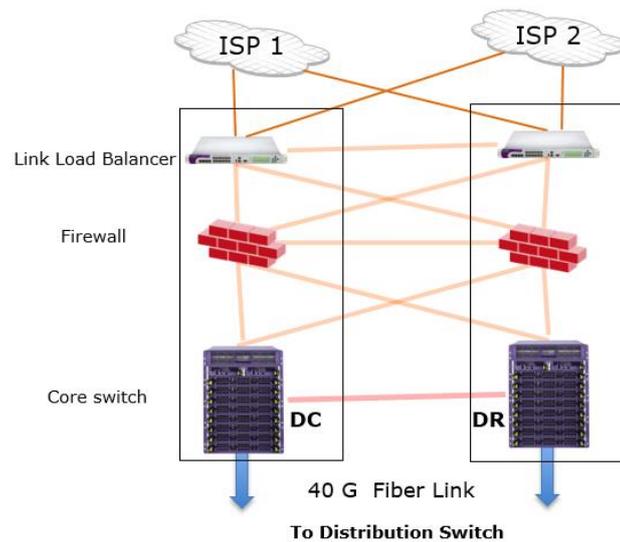
Figure.5 : Criss cross connections between DC and DR

V. RESULTS AND DISCUSSION

4.1 Users and Devices

Users and devices have been loaded on this network via wired and wireless connections. A controller based WiFi infrastructure has been loaded and about 100 wireless users and IoT devices are connected concurrently. The VOIP, Surveillance system and Servers have also been loaded. The utilization of ISPs have been observed and the graphical representation is given in figure 6. It was noticed that the ISP utilization from both the ISPs are happening in an effective manner in active – active mode. It can be seen from the figure that the system is stable and provides seamless connectivity even thoughout the period even though the usage was heavy.
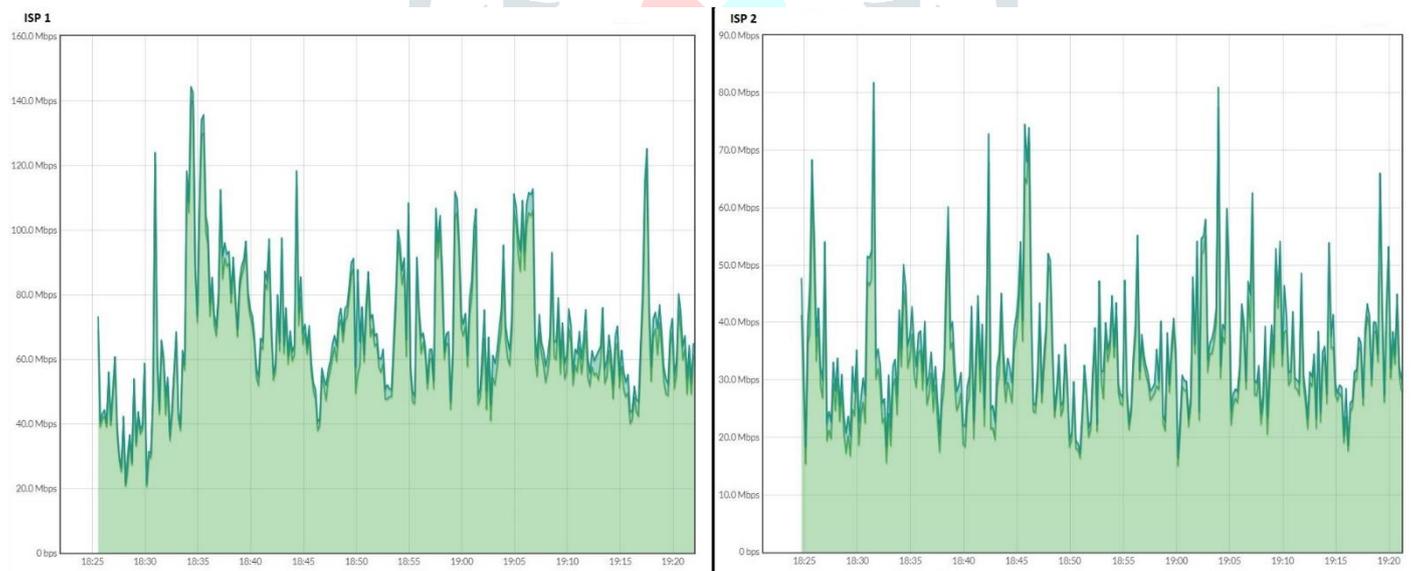

Figure.6 : Utilization graph of ISPs (Y axis- bandwidth and X axis : Time)

This is also observed that the memory utilization is not going beyond 50% which indicates the stability of the system. The usage level was 43 % which proves that the system is capable of handling heavy load with the available resources. The memory utilization graph is given in figure 7. The session rate has also been shown in this graph which shows the capability of the system for opening concurrent sessions without causing any stability issue.
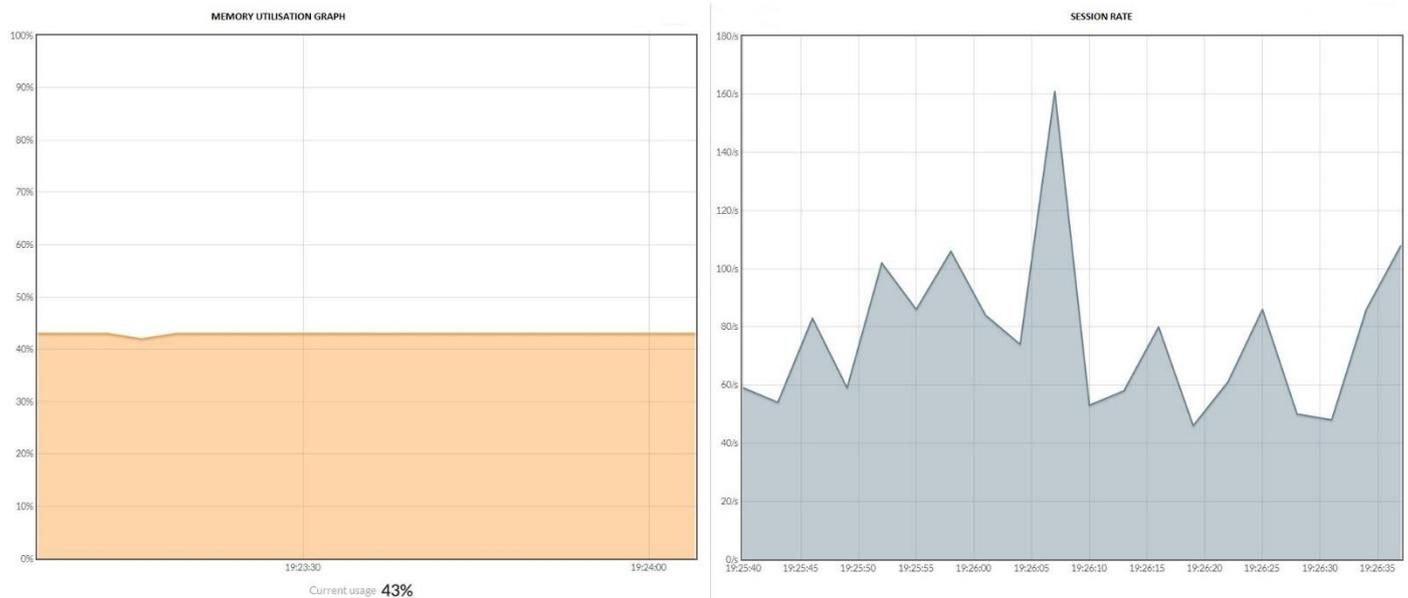
Figure 7: Memory utilization and session rate

V. CONCLUSION

The challenges in designing the network infrastructure have been increased due to the technology changes caused as an outcome of the drastic increase in the usage of online applications through the network infrastructure. Having a network that is responsive and able to adapt is important to keep up with the demands placed upon it. A backbone is required so that the people with all their devices can roam and stay connected. The present model exhibits the best practices to be followed for establishing a state of the art network infrastructure in an enterprise campus for any mission critical application with 24/7 working environment.There are multiple strategies applied in this paper for the implementation of the network infrastructure. According to the requirement of the institution and geographic conditions there would be variations from this model.

REFERENCES

[1] S. Zubair , Y. A. Adediran, S. Misra, B. A. Salihu, H. T. Abdulazeez and A. Suleiman. 2011. Effect of network hierarchy in a typical campus area network (CAN) of a university, Scientific Research and Essays 7(6): 627-635.

[2] Marwan Al-shawi published by Cisco Press. 2016. Campus Network Design Models, https://www.networkcomputing.com/data-centers/campus-network-design-models

[3] Matt Conran, 2018. A new era of campus network design, https://www.networkworld.com/article/3281447/lan-wan/a-new-era-of-campus-network-design.html

[4] Juniper networks. 2017. Midsize Enterprise Campus Design, https://www.juniper.net/documentation/en_US/release-independent/solutions/information-products/topic-collections/midsize-enterprize-campus-ref-arch/topic-94264.html#jd0e174

[5] Xingyu Li and Tingting Jiang. 2014. Design and implementation of the campus network monitoring system, IEEE Xplore Digital Library, IEEE Workshop on Electronics, Computer and Applications

[6] Juniper networks. 2014. Juniper Networks Enterprise Wan Solution Architecture https://www.juniper.net/documentation/en_US/release-independent/solutions/information-products/pathway-pages/solutions/8030013-en.pdf

[7] David Hucaby, Denise Donohue, and Sean Wilkins, published by Cisco Press. 2010. Campus Network Design, Network world, https://www.networkworld.com/article/2243250/lan-wan/chapter-1--campus-network-design.html

[8] Cisco System Inc. 2008. Campus Network for High Availability Design Guide, https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

[9] Cisco - Design Zone for Enterprise Networks, Design Zone for Campus Wired and Wireless LAN, https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html

[10] Cisco System Inc. 2002. Introduction to Cisco Network Design, http://www.ciscopress.com/articles/article.asp?p=25259

[11] S.L. Sanjith and E George Dharma Prakash Raj. 2018. A Comprehensive Analysis of Machine Learning Models for Real Time Anomaly Detection in Internet of Things, International Journal of Computer Sciences and Engineering 6(11)