Modern Data Center Design

A dissertation submitted to the

Dept. of Electronics and Communication Engineering

EAST WEST UNIVERSITY

For the Degree of
B.Sc in Electronics and Telecommunication Engineering

SUBMITTED BY:

Name: MD.Robiul Islam

ID: 2012-2-55-055

Supervised by:
Dr.Nahid Akhter Jahan
Assistant Professor
Dept. of Electronics and Communication Engineering
East West University

DECLARATION

We hereby declare that we carried out the work reported in this project in the Department of Electronics and Communication Engineering at East-west Universityunder the supervision of **Dr.Nahid Akhter Jahan**. I solemnly declare that to the best of our knowledge,no part of this report has been submitted elsewhere for award of a degree.All sources of knowledge used have been duly acknowledged.

Signature:

…………………………………

MD.Robiul Islam

ID:2012-2-55-055

APPROVAL

This is to certify that the project titled as ‘Modern Data Center’submitted to respected members of the Board of Examiners of the Faculty of Engineering for partial fulfillment of the requirements for th**e** degree of Bachelor of science in Electronics and Telecommunications Engineering by the following students and has been accepted as satisfactory.

Submitted By:

MD.Robiul Islam

ID.2012-2-55-055

……………………………………… ………………………………………………

Dr.Nahid Akhter Jahan Dr.Mofazzal Hossain

Assistant Professor Chairperson and Professor

Dept. of Electronics and Communication Engineering Dept. of Electronics and Communication

East West University Engineering

East West University

Acknowledgements

All praise and thanks to almighty Allah who is our creator, sustainer, nourisher, protector and curer. May His choicest of blessings and salutations be upon our beloved prophet Muhammad ṣallā Allāhu ʿalayhi wa-sallam, his family members, his companions, and all those who follow his path with utmost sincerity until the Day of Judgment.I would like to express my sincere gratitude and appreciation to my respected supervisor **Dr.Nahid Akhter Jahan** for his continuous encouragement, technical suggestions and valuable instructions throughout the academic journey.I would also like to thank all the honorable teachers of the Department of Electronics and Telecommunication Engineering, of East-West University for their inspirations and advices.I am also thankful to the laboratory staffs of our department for their fast response and cooperation.And at last but not the least a big thanks goes to my parents for their constant support and encouragement throughout the study period.

The author

CONTENTS

ABSTRACT

The main objectives of this project is to study different criteria and requirements to design a modern data center for any organization .This provide a standard solution to create a Data Center for an organization to consolidate the services, application and it's IT infrastructure. A Data Center is a place that centralizes an organization's IT operations and equipments, and where it stores, manages it's data. Data centers house a network's most critical systems and are vital to the continuity of daily operations. The data center network design is based on a proven layered approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. Throughout the internship I have learned pertinent aspects concerning data center design and its proper maintenance. By dint of this opportunity I have gained the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance. I believe this experience have enriched by knowledge towards a better future.

Chapter 1

Introduction

1.1 Data Center: An overview:

A Data Center is a place that centralizes an organization's IT operations and equipment, and where it stores, manages its data. Data centers house a network's most critical systems and are vital to the continuity of daily operations.The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered. Another important aspect of the data center design is flexibility in quickly deploying and supporting new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant competitive advantage. Such a design requires solid initial planning and thoughtful consideration in the areas of port density, access layer uplink bandwidth, true server capacity, and oversubscription, to name just a few.

The data center network design is based on a proven layered approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. The layered approach is the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance.

1.2 Data Center Tier :

Tier of data center is nothing but a standardized methodology used to define uptime of a data center. This is useful for measuring availability, performance and investment.

There are 4 Tier level of data center.They are like follows,

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity data center components • 28.8 hours down time per year • Data center availability is 99.671% • Used by small organizations
2	• Meets or exceeds all Tier 1 requirements • Redundant of server, power and HVAC. • 22 hours down time per year • Data center availability is 99.741% • Used by Medium size organizations
3	• Meets or exceeds all Tier 2 requirements • Multiple independent distribution paths serving the IT equipments and all IT equipment must be dual-powered • 1.6 hours down time per year. • availability is 99.982% • Used by large size organizations
4	• Meets or exceeds all Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating. • Fault-tolerant site infrastructure with electrical power storage and distribution facilities. • availability is 99.995% • Used by Enterprise Corporations

In design concept, two types of Data Center.

They are:

1. Traditional Data Center
2. Modern Data Center

1.3 Features Traditional Data center:

- One Server per physical host
- Proprietary and not customized
- Limited Capacity
- Mixed hardware environment
- Huge procurements and provisioning issues
- Long Time consuming process
- Frequent application patching and updating
- Complex workload
- Capital Expenditure is very high
- < 15 % Resources are Utilized
- Less Secure
- Require very high power, space and cooling systems.

Traditional designs almost always intentionally incorporate excess capacity upfront because subsequent expansion of power and cooling capacity is extremely difficult and costly in a production data center. This often has the effect of people being overly conservative in capacity planning which then results in higher upfront capital costs and a chronically inefficient data center. The proper deployment of facility modules, on the other hand, eliminate this wasteful over sizing tendency, because its standardized, modular architecture makes adding or reducing capacity to meet real-world, dynamic demand much easier. This, in conjunction with efficient, integrated power and cooling technologies results in TCO savings of 30% compared to a typical oversized data center operating today.

1.4 Features Of Modern Data Center:

- Many Servers per Single Physical Host
- Huge Cost Savings
- Minimal application patching and updating
- Simple workloads
-
- > 70% Resources are utilized
- Easy procurement and provisioning issues
- Less time consuming process to acquire compute, storage, network and services.
- More Secure
- Customizable
- Near to unlimited capacity
- Less power, space and cooling

The Consideration elements for a Modern data center design breakdown as follows:

1. Standard and regulation for modern Data Center
2. Site Selection
3. Space Design
4. Network Topology
5. Network Architecture
6. Network Infrastructure
7. Network cabling
8. Network Design
9. Virtualization
10. Power Supply
11. Cooling system
12. Fire protection
13. Security
14. Monitoring
15. DISASTER RECOVERY

1.5 Standard and regulation for modern Data Center:

The successful and reliable provision of modern data centre services depends upon the following issues;

• A well designed and constructed plant that takes into account appropriate Standards and best practice to achieve efficient and reliable operation .

• Management techniques that put in to place operating procedures and protocols that ensure the continuing efficient and reliable operation of the data centre.

• Disaster recovery plans that have an established and rehearsed procedure for dealing with any incident that impairs the operation of the data centre and puts in to place a recovery programmed.

1.6 Technical Standards for data Center:

Technical Standards give the best practice methods for designing and implementing the data centre from a physical, electrical and mechanical viewpoint. Some requirements covering health and safety and energy management are covered by European Directives and national standards. Many technical standards exist that cover the myriad of engineering disciplines encountered in a data centre but the main documents drawn upon in this Standard are;

ANSI/TIA-942:2010 Telecommunications Infrastructure Standards for Data Centers .
The Up Time Institute, 2010 Tier Classifications define site infrastructure performance.

ASHRAE TC 9.9 2011 Thermal Guidelines for Data Processing Environments – Expanded Data Center Classes and Usage Guidance .

ISO/IEC 27001:2005 Information technology.

ANSI/TIA/EIA568-C Commercial Building Telecommunications Cabling Standard iscomposed of several sections related to both systems and components.

568-C.0 - LAN Topology, Grounding and Bonding, Cable Installation, Polarity of FiberSystems, Cable Transmission and System Testing Requirements.

568-C.2 - Balanced Twisted-Pair Telecommunications Cabling and Components Standards.

568-C.3 - Optical Fiber Cabling Components Standard.

Chapter 2

2.2 Geographic location :

First and foremost factor is the geographical location of the site. This has to be thought out at the outset. Few things which needs to be looked are: Natural disasters (Earth quake, Flood, Rain, Cyclones etc.) – probability and frequency of occurrence at the said location; Environmental hazards – Impact and degree of affect; and Climate – Climates which support free cooling (outside air cooling) will be an added advantage.

2.3 Construction :

While building a data center at any particular location, construction cost and options play a major role. Following aspects should be considered for making a decision: Construction industry maturity, experience, process in place and technology availability at the considered site; and Labour – Availability and cost of labour at the considered place.

2.4 Availability of electricity power:

Electricity or power is important factor as it is one of the chief constituent to operating cost of a facility. we need to understand. Factors include: Availability – While looking at availability of electricity, we need to weigh options like access to more than one grid, maturity of grid, various generation options, power transmission mechanism, etc.; Cost – Need to compare cost of electricity across various options. i.e. it should have low cost and Alternative source of power – Management can look into renewable energy options like solar, wind, air etc. which will help company to become greener.

2.5 Availability of telecommunications infrastructure:

Telecommunication is one of the most important components for a datacenter. While selecting a site for datacenter, various factors need to be considered with respect to telecommunication infrastructure perspective. Following list will help in this regard: Fibre backbone route and its proximity – How near a fibre backbone to the selected site. It will help to gauge addition investments required from backbone route to the exact data center location; Type of fibre – Will affect speed and transmission; Carrier type and support – What all carriers are present in the vicinity and their support & service model in place; and Latency – Transaction time/latency will be an important factor.

2.6 Cost of utilities:

While selecting a site for modern datacenter, various utilities cost need to be consideration. Those Utilities are like natural gas,water,electricity,telecom,transportation etc. Cost of utilities must be cheaper as possible.

2.7 Labor costs and availability:

Labor costs and availability are one of the important issue for selection of data center location. before selection of any location, we have to consider labor costs & its availability. it should be reasonable then other location. Otherwise TCO will be very high.

2.8 Transportation **:**

Availability and proximity of various modes of transportation affects site selection for a data center, as equipment must be delivered and workers must commute to the location and vendors must visit it.

2.9 Cost of living :

Presence of various day to day requirements and cost of living is an important factor which has to be though/analyzed while selecting a site by a company.

Chapter 3

Floor Plan:

3.1 Floor Space Design:

Floor space in a data center is normally divided between space for servers and network gear, and space for operators and managers. Modern computer and networking equipment is much smaller than legacy equipment, so data center floor space requirements have tended to shrink over the last few years. However, your situation will require careful analysis. It's always better to have too much space in your data center than too little.

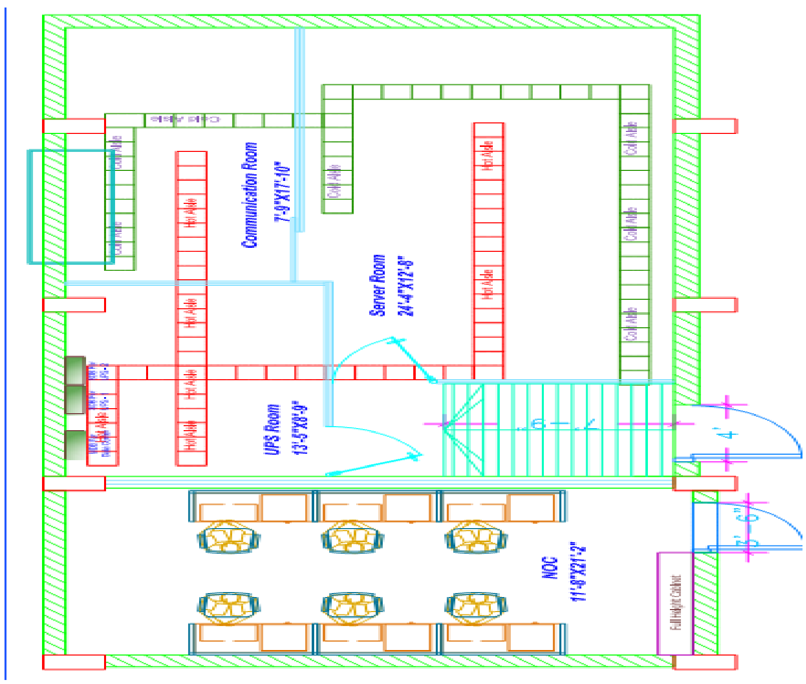

Figure 3.1: Floor Design

3.2 Aisle, Racks and Cooling Dimensions :

In calculating the floor space required for the data center you not only have to calculate the dimensions of all the racks and equipment to be placed in the room; you must plan space for aisles, ramps and the cooling requirements of the racks. Aisle space must be wide enough for racks to easily be brought in and out without touching or moving other racks in the room. Careful consideration needs to be taken with any special clearance requirements for electrical panels, fire suppression systems, cooling devices, rack door openings (for enclosed racks) and room to perform maintenance on the devices within the racks as some are designed to slide out into the aisle for maintenance access. There should also be several breaks in the rows across the room to allow for the efficient maneuvering of racks and people throughout the data center. Depending on equipment type used, the need for dock access and sufficiently sized entry points needs to evaluated. If the data center is to reside above the main floor, elevator size and opening dimensions will play an important part in any equipment delivery and usage.

In addition to the rack's width and depth dimensions, the cooling requirements of the enclosed rack must be considered. Most racks pass air through them for the cooling of the equipment they contain. Some racks pass cool air in from one side and exhaust out the other. This type of rack typically requires several inches of clearance on either side to accommodate proper airflow. Many racks pass air from front to back or from bottom to top, allowing the racks to be placed right next to each other. This is a more space efficient design and should be considered when choosing a rack.

Different sizes of racks are also available, varying in width and depth depending on the type of equipment they will contain. To avoid wasted space, equipment that is too large to fit in the standard 19" rack (22" W x 80" H x 30" D) should be placed together in the same racks and area of the data center. Equipment that is not rack-mountable, such as large disk arrays, DLTs, and stand-alone server and network devices, should be similarly placed. A simple diagram, done on a grid of your floor-tile layout, will go a long way to helping position your equipment for the best possible use of floor space.

Typical free floor space for a well-designed data center is from 40 to 50 percent of its total square footage.

3.3 RAISED FLOORING :

Figure 3.2 : Raised Floor.

Raised flooring is, by far, the most popular choice in data center design for many reasons. It gives you the most flexibility for network and electrical cabling and HVAC (Heating, Ventilating and Air Conditioning) air flow system design. Raised floor cooling systems are also typically cheaper and require less electricity than open-air cooling systems, as only the air beneath the floor and within the racks needs to be cooled. With an open-air cooling system, the temperature of the entire room must be controlled, requiring

more capacity in the air-handling system. A raised floor is typically built 24 inches off the ground with the surface made up of two-foot square tiles. These tiles can be removed and replaced to allow access to wiring that may lie beneath. Strategically placed grated or perforated tiles allow for controlled airflow to cool the racks. Cable trays for all the cabling that will run under the floor need to be well thought out and planned in advance.

They should be installed above the main flooring to keep the cables out of any potential flooding and meet any special requirements there may be for the type of cables being run, such as fiber.

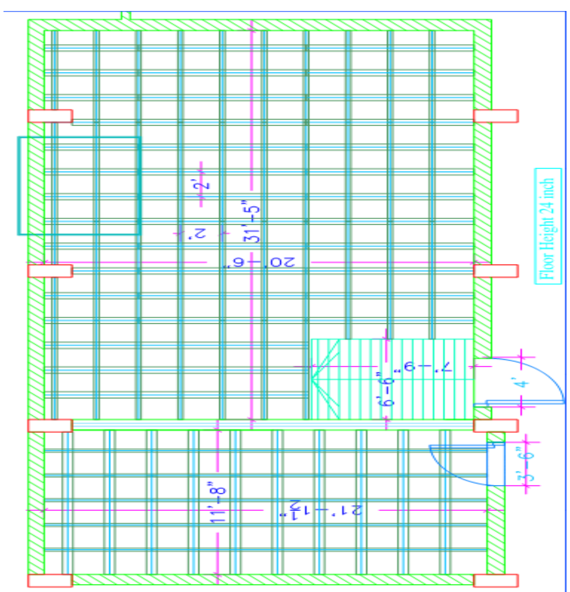

Figure 3. 3: Raised Floor Design

When all the tiles are in place, you can't easily see what is going on underneath. One concern is the possibility of flooding. Moisture/water sensors must be placed under the flooring to detect this. These sensors usually run SNMP and can tie into your monitoring solution. Fire suppression systems should also be deployed under the raised floor, as the smoke from a fire could go undetected by ceiling-mounted smoke detectors, or possibly consumed directly into the air handling system.

3.4 Floor Load Planning :

Weight is a very important factor to consider when designing a data center. Incorrect or incomplete calculations could spell disaster.

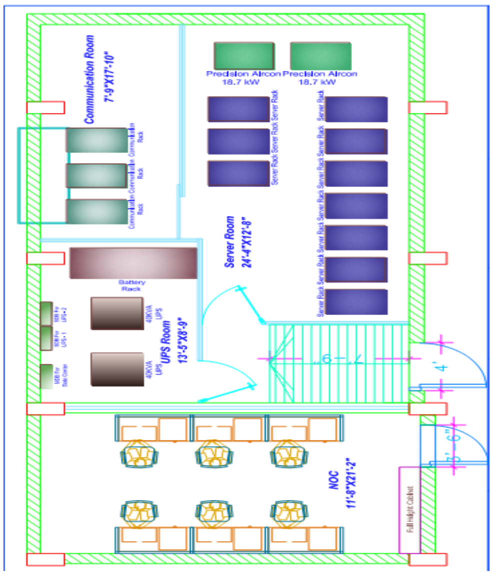

Figure 3.4 : Floor Planning

3.5 Entire Floor Load :

The first factor to consider is the total weight of the entire floor. The weight of all the racks and other equipment, current and future, must be calculated. This is especially important to consider when the data center is not going to be on the ground floor of the building. You must consult with your building’s design to determine its maximum weight capacities. Don’t forget to calculate the weight of the raised floor itself when figuring floor load; floor tiles and the load-bearing framework that hold them are very heavy.

3.6 Tile Load Capacity :

There are different types of tiles, each with a different load rating. The capacity of the tile must exceed the weight placed upon it. With racks that have casters, it is important to think of the point load capacity of the tile when planning. The point load of a rack is its weight at any one of its casters. Because it is possible that two casters, from two different racks, could rest on the same time, you need to double the point load value when figuring tile load capacity requirements. The load capacity of the tile that is chosen should exceed one half the weight of the room's heaviest rack.

Chapter 4

Data Center Network

4.1 Network Topology :

Simply defined, a network is a communication system that seamlessly and efficiently connects voice, data, video and other selected applications together. Network speed and complexity have increased over the past 40 years and certain standards emerged out of the various protocols that were created, called topologies.

The discussion of cabling topology covers two types of topologies: physical and logical.

Physical topology is the way cabling or media is installed and connected to the devices.

Logical topology is the way information travels on the cabling or media.

A network's logical topology is not necessarily the same as its physical topology. For example, twisted pair Ethernet is a logical bus topology in a physical star topology layout. While IBM's Token Ring is a logical ring topology, it is physically set up in a star topology.The best physical topology, as recommended by the standards, is a star configuration. Using a physical star, it is possible to implement any logical topology.

4.2 Network Physical Topologies

Star Topologies

In a physical star topology, network devices are cabled to meet at a point of concentration, usually a piece of active electronics called a hub, router, switch or node. These actives are then connected to an intermediate point of concentration, and so on, until all traffic meets at a central point.Logical buses, rings and stars can be cabled together into a physical star. The hierarchical and centralized nature of the star permits the easy concentration of cables and components, thus easing maintenance burdens. Network additions can be accommodated easily by a physical connection at any of the collection points. TIA and other standards typically recommend a physical star topology within buildings.

Ring Topologies

In a physical ring topology, the nodes of a network are all connected in a closed loop. Instead of running back and forth between nodes, the signal travels in one direction around the ring. In some networks, active and stand-by parallel circuits operate in both directions simultaneously (a counter-rotating ring). Rings are normally used in the campus backbone segment of a network. Their advantage is that if a cable is cut or a node fails, the network will continue to operate. However, adding more nodes to the ring is difficult. Trying to adapt bus or star logical topologies to a ring may result in unacceptable connection loss.

Mesh Topologies

In a physical mesh topology, every device or node is connected to every other device or node in the network. Adding a device or node requires multiple connections.

4.3 Network Logical Topologies

Bus

Defined under IEEE 802.3, this is a popular protocol in which signals travel in both directions on a common path. In most 802.3 systems, collision detection software in the active equipment directs the traffic so that network subsystems do not try to send and receive at the same time. Common bus protocols include the Ethernet family and MAP (Manufacturing Automation Protocol).

Ring (also called Token Ring)

Defined under IEEE 802.5, signals travel in one direction on one path and the oppositedirection on another (a counter-rotating ring). A ring’s advantage is reliability - if the connection should be cut or a node fails to function, the ring bypasses the failed component and continues to operate. Another version of a ring is FDDI (Fiber Distributed Data Interface defined under ANSI X3T9) written specifically for optical fiber.

Star

In a star, all of the components connect into a central node that distributes the traffic back out. Most private telephone networks are star topologies. Terminal/mainframe computerconnections are normally star topologies as well.

Mesh Topology

Devices are connected to every other device in the network. In a true mesh topology every device has a connection to every other device in the network.

Point-to-Point

This is the simplest type of connection, linking a minimum of two devices over a transmit/ receive link. CCTV, Fibre Channel, ESCON and VSAT (and other satellite antenna links) are point-to-point topologies.

4.4 Network Architecture

Network architecture is the layout of the cabling infrastructure and the way the various switches are connected. We will first discuss the switching methods.

Switches There are three different types of switches commonly used: Core, distribution and access Network Switch

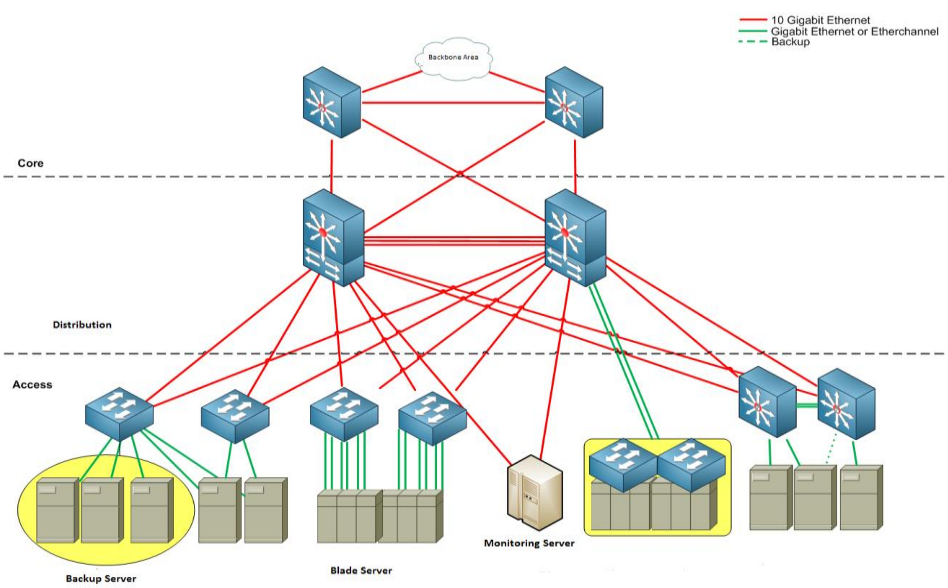

Figure 4.1 : 3 Layard Network of Data Center

4.5 Core Switch

A core switch is located in the core of the network and serves to interconnect edge switches. The core layer routes traffic from the outside world to the distribution layer and vice versa. Data in the form of ATM, SONET and/or DS1/DS3 will be converted into Ethernet in order to enter the Data Center network. Data will be converted from Ethernet to the carrier protocol before leaving the data center.

4.6 Access Switch

An access switch (also called an edge switch), according to Newton's Telecom Dictionary, is a Broadband Switching System (BSS) located at the edge of the network. An edge switch is the first point of user access (and the final point of exit) for a network. Also known as the access switch, an edge switch will allow the servers to connect to the network. Multimode optical fiber is the typical media that connects the edge devices to the servers within the data center. Edge switches are interconnected by core switches.

4.7 Distribution Switch

Distribution switches are placed between the core and edge devices. Adding a third layer of switching adds flexibility to the solution. Firewalls, load balancing and content switching, and subnet monitoring take place, aggregating the VLANs below them. Multimode optical fiber will be the typical media running from the distribution layer to the core and edge devices. Not every data center will have all three layers of switching. In smaller Data Centers the core and distribution layer are likely to be one and the same.

Chapter 5

Data Center Infrastructure

5.1 Data Center Equipment:

The Data Center is basically a large computer room which houses a mixture of active andpassive equipment.

5.2 Network Server:

A server is a combination of hardware and software that provides applications, such ascorporate e-mail and webhosting, to client computers. Although a server has much of thefunctionality of a laptop computer, advanced in CPU and memory technology allow servers to be significantly more powerful, running multiple operating systems and applications. The traditional server is often described as a ” box” because of its shape; it is 1U in height and is mounted into a rack. These are also known as “rack optimized” servers, as they were originally compared to tower servers, which were not optimized for racks. A blade server is designed to minimize space by stripping redundant components common to most servers, such as the power source, network ports and management interfaces. A server blade can be mounted into a chassis backplane that will have a consolidated group of all the components that each individual blade server is missing, leaving only the raw computer and memory in a fraction of the space. In addition to reduced cost per server, blade servers are modular and can be added one blade at a time. They also draw less power per physical server, and in turn generate less heat overall.

Traditionally, each server has been used to run a single application. This has proved somewhat inefficient, as a server is capable of running multiple applications simultaneously without loss of performance. Running two applications on one server could reduce the number of servers needed by 50%, and running a higher number of applications per server could reduce the physical devices needed even further. Running multiple operating systems on one physical server is known as virtualization, where a new application can be added onto a virtual “machine” instead of adding a new physical device.

The benefits of virtualization include reducing the energy, heat dissipation, and requiredcabling, as well as a potential reduction in management and maintenance costs. Putting more “eggs in one basket” does make operation and connection to the remaining servers more critical. Virtualization is leading to the use of higher grade cabling to handle the increased expectations for data traffic to and from that server.

5.3Blade Server

Blade systems (blade, blade server, blade center) are one of the most modern server designs and are the fastest growing segment of the server market.

However, they do not differ from traditional rack servers in terms of operation and the execution of applications. This makes it relatively easy to use blades for software systems that already exist. The most important selection criteria for blade servers are the type of application expected to run on the server and the expected workload. In consideration of their maintainability, provisioning and monitoring, blades on the whole deliver more today than their 19-inch predecessors, yet are economical when it comes to energy and cooling. For example, a Blade

Center, an IBM term, provides the infrastructure required by the blades connected inside it. In addition to the power supply, this includes optical drives, network switches, Fibre Channel switches (for the storage connection) as well as other components.

Figure: Blade Server

The advantage of blades lies in their compact design, high power density, scalability and flexibility, a cabling system that is more straightforward with significantly lower cable expenditure, and quick and easy maintenance. In addition, only a single keyboard-video-mouse controller (KVM) is required for the rack system.

A flexible system management solution always pays off, especially in the area of server virtualization. Since in this situation multiple virtual servers are usually being executed on one computer, a server also requires multiple connections to the network. Otherwise, one must resort to costly processes for address conversion, similar to what NAT (Network Address Translation) does. In addition, the level of security is increased by separating networks. Many manufacturers allow up to 24 network connections to be provided for one physical server for this purpose, without administrators having to change the existing network infrastructure. This simplifies integration ofthe blade system into the existing infrastructure.

5.4 Network Switch:

A switch is a networking device that connects multiple segments together and typically operates at Layer 2 (data link layer) of the Open Systems Interconnect (OSI) model. A switch not only creates a network to transfer data between individual components, but it can also be used to segregate the data in transport to create separate collision domains called virtual LANs, or VLANs. For example, the switch can connect a grouping of equipment running at 1 gigabit Ethernet to the backbone network operating at 10G speeds and differentiate between these two networks as it handles traffic. If the switch has additional functionality to process data, then it may also operate at Layer 3 (network layer).

5.5 Network Router:

A router is a device that connectors multiple networks together, typically at Layer 3 (network layer) of the OSI model. Acting as a gateway, a router can connect networks of different protocols, such as ATM to Ethernet at the core routing area of the data center. Because of their position at the edge of each network, routers often have firewalls and other complimentary capabilities integrated within them.Access to storage can be organized in several ways. Legacy systems used Direct AttachedStorage (DAS) before storage devices became attached to a network. DAS is simplyconfigured where there was a direct cable link between the server and one (or more) storage devices. The main protocols used for DAS connections are ATA, SATA, SCSI, SAS and Fibre Channel. This network may be easy to configure, but lacked scalability and redundancy, and is now typically reserved for legacy systems or areas of limited expected need or growth.

5.6 Storage Area Network (SAN):

For a more dynamic and scalable architecture, a Storage Area Network (SAN) can be created which will allow servers to access data from multiple storage devices, running over multiple paths for redundancy and speed. About 90% of the networked storage within the data center is run over a SAN. In this architecture, remote computer storage devices (such as disk arrays, tape libraries and optical jukeboxes) are attached to servers in such a way that the devices appear as locally attached hard drives to the operating system. Fibre Channel is the typical protocal used in the SAN and optical fiber is the typical cable media. Less common than SANs, Network-attached storage (NAS) is used on the LAN side for file storage and operates over IP-based Ethernet; copper cabling is the typical media. NAS is utilized in networked storage environments that do not require the service level paramenters of FC such as networked home directories or department file-sharing. NAS in essence is a large file server, usually having backend SAN fiber connections and translating FC storage to IP traffic.

Tape storage devices were introduced almost 60 years ago and they have continued toimprove over time with regards to size, cost and reliability. Data transfer speeds of up to120MB/s are available today. Disk technology is newer and often perceived as having higher performance, as disks devices are available for fast access. Tapes are generally stored inert after data has been transferred to them, and have to be loaded when data access is required.Tape storage has maintained a cost advantage over disk, and is therefore often the choice for back-up, recovery infrastructure or data with low-access requirements. Both types of storage are widely used today, often within the same data center.

There are many options for the storage devices themselves. These devices may comepreassembled in their own housing or cabinet. This saves time and installation headaches, but there may be better cabinet options for power and cooling if ordered separately.Servers are typically housed in cabinets that are 600 - 800 mm wide by 800 - 1000 mmdeep, although it is not uncommon to find 1200mm deep cabinets to support high-densityserver applications that exhaust higher heat loads.

Within the cabinet is a 19 inch wide rack that the servers can be mounted to. Although a rack may have the physical capacity to support up to 44 (or more) 1U servers, there are many practical limitations to consider, such as weight, power supply, heat dissipation and cable management. A typical cabinet will house 10–15 servers; while a cabinet prepared for high density may house 20–25 servers. Server cabinet density is typically measured in terms of watts per rack. This allows Data Center designers to adequatly allocate proper power and cooling for short-term needs and long-term growth.

Network cabinets are expected to hold more of the passive patching and are offered inwidths of 600 mm to 1000 mm with a depth of 800 mm to 1200 mm. Network cabinets are capable of supporting a mix of patching and electronics with a weight capacity of 1100 lbs (compared to 2200 lbs for a typical server cabinet). LAN & SAN switches can weigh 200 to 300 lbs each with a typical density of 2 per cabinet. This weight, plus that of the copper and/or fiber cabling, will typically not exceed that 1100 lb limitation.

The chassis for a blade server will take up much more space than the typical 1U server.Configurations differ, but as an example, a single chassis that can hold 16 blade servers may take up 10U of space, allowing for a total of four chassis and 64 blades servers within one cabinet. When filled out, this is a higher density than available with 1U servers. However, the 10U for each blade server is lost space, even if the chassis is not filled out. In an IBM mainframe solution, a director (switch) is commonly its own separate entity, thus taking all the guesswork out of filling a cabinet. However, it is important to note that the power and cooling capacity can support a fixed number of mainframes in a given area, thus dictating their placement.

From a cabling point of view, mainframes are generally wired from under floor. They usually don't have any suitable locations within their cabinets to mount structured cabling panels or shelves, so floor box consolidation boxes are popular in such environments. Another approach is to use a cable consolidation cabinet in proximity to the mainframe cabinets to facilitate the same sort of cabling support.

5.7 Network Interface Card

A network interface card (NIC) usually exists "onboard" a network-compatible device and creates the physical connection to the network, by means of an appropriate access method. Ethernet in all its forms (different media and speeds) is currently being used almost exclusively as an access method, also known as a MAC protocol

(Media Access Control).

Each NIC has a unique hardware address, also called a MAC address, that is required by switches in order to forward Ethernet frames. The first 3 bytes of this 6-byte MAC address is assigned by IEEE for the manufacturer, who uses the remaining 3 bytes as a serial number. Therefore, in addition to its configured IP address which is required for routing, every device integrated in an Ethernet LAN also possesses a MAC address, which is used by switches for forwarding.

5.8 Firewall

A firewall is a software component that is used to restrict access to the network on the basis of the address of the sender or destination and services used, up to OSI layer 7. The firewall monitors the data running through it and uses established rules to decide whether or not to let specific network packets through. In this way, the firewall attempts to stop illegal accesses to the network. A security vulnerability in the network can therefore be the basis for unauthorized actions to be performed on a host.

A distinction is made, on the basis of where the firewall software is installed, between a personal firewall (also known as desktop firewall) and an external firewall (alsoknown as network or hardware firewall). In contrast to a personal firewall, the software for an external firewall does not operate on the system to be protected, but runs on aseparate device (appliance) which connects the networks or network segments to one another and also restricts access between the networks, by means of the firewall software.Other firewall functions include intrusion detection and prevention (IDP), which checks the data transfer for abnormalities, as well as content/URL filtering, virus checkingand spam filtering. High-end devices use these functions to check data transfers up to 30 Gbit/s.

5.9 Twisted Copper Cables (Twisted Pair)

In designing a data cabling system in modern data centers that is geared for future use, there really is no alternative to using twisted pair, shielded cables and connectors.

This is not a big problem for cabling systems in the German-speaking world, since this is already a de facto standard for most installations. The possibility also exists to choose your required bandwidth from the large selection of shielded cables and connectors (note: Category 6 or 6A are also available in an unshielded version).Cabling components based on copper (cables and connecting elements) can therefore be differentiated as follows:

· Category 6 (specified up to a bandwidth of 250 MHz)

· Category 6A / 6A (specified up to a bandwidth of 500 MHz)

· Category 7 (specified up to a bandwidth of 600 MHz)

· Category 7A (specified up to a bandwidth of 1,000 MHz)

5.10 Optical Fiber Cable:

Optical fiber cabling systems is one of the most important part of modern data center for speedy and faster communication. Fiber optic cables are essentially very thin (125 microns or µm) strands of glass that propagate light in an even smaller diameter core. Multimode fibers have (relatively) larger diameter cores (50 and 62.5 µm) that permit light to travel over hundreds of (or multiple) modes, or paths. The smaller core of single-mode fiber permits only one path (a single 'mode').

Advances in connector technology have made fiber easier to work with. Media converters are needed in order to interface with copper cabling or electronics that connect to them. However, fiber's low attenuation and superior bandwidth makes it an obvious choice for backbone and campus links. Although there is a trade-off with the higher cost of electronics, single-mode cables have the highest performance and can be used for links of 70 km (43.5 miles) and longer.

Fiber optic cables need to conform to basic physical and performance standards that are

stated by TIA/EIA, Telcordia, ICEA and others. These govern the mechanical, environmental and optical performance of the fiber. In a multimode fiber, the higher the number of modes, the greater the modal dispersion (when light pulses 'spread out' and become unrecognizable by the receiver as individual pulses). Low modal dispersion results in higher bandwidth. Bandwidth will be specified and will be a limiting factor in the data rate and distance used with this media Single-mode fiber has only one mode and does not experience the modal dispersion seen with multimode fiber. The bandwidth for single-mode fiber is not normally specified as it is not stressed by today's electronics. Instead, attenuation and non-linear effects determine the distances used in single-mode systems.

5.11 External Network Connectivity:

The main planning issues involving network connectivity for modern data centers are capacity and redundancy.Capacity refers to the total network bandwidth into and out of your data center. This is usually expressed in megabits per second.

T-1 1.544 Mb/s

E-1   2.0 Mb/s

T-3 44.75 Mb/s

OC-3 155 Mb/s

Network redundancy is provided both by selecting network providers that offer highly redundant network connectivity, and by selecting multiple network providers.

Network redundancy can be planned on a symmetrical or asymmetrical basis. An example of symmetrical network redundancy would be provisioning a T-3 circuit from one Tier-1 provider and a T-3 circuit from another Tier-1 provider. An example of asymmetrical network redundancy would be provisioning a T-3 circuit from one Tier-1 provider and a T-1 circuit from another Tier-1 provider. Network redundancy can be active-active or active-passive. Active-active network redundancy is significantly preferable. Active-active redundancy means that both circuits are constantly up and passing traffic. Active-passive redundancy means that the backup circuit only becomes operational when the primary circuit fails. Active-passive redundancy is used to provideredundancy at a lower cost. Active-active redundancy provides more total bandwidth. Active active redundancy is also superior because the backup circuit is constantly being tested.

However, there is one major planning step to be aware of when utilizing active-active network redundancy. If your data center network capacity requirements are 2.5Mb/s, and you provide that with two T-1 lines – you do not have network redundancy. In the event of an outage of one of your circuits your total network capacity will be 1.544Mb/s. To provide effective network redundancy, you will need to provision at least three T-1 circuits from three different providers, or four T1s, two each from different providers.Active-active redundancy is normally enabled through the use of the BGP4 (Border Gateway Protocol 4) routing protocol.

Another important issue in provisioning network capacity for your data center is performance, which is often measured in latency. A 1.544Mb leased line will have much better performance (i.e. lower latency) than a 1.544Mb satellite link. When purchasing bandwidth, the Internet routing model, ISP-to-customer routing model, private and public peering relationships, and type of SONET technology being used by potential providers should all be taken into account. In addition, you often have to worry about network congestion caused by oversubscription on the part of your network provider. If they are selling T-1s to fifty customers, and they only have a single T-3 upstream to their provider, you may not actually see 1.544Mb of throughput on your T- 1 circuit. This information is often difficult to locate; a thorough investigation of news and eventsabout the provider can usually be found online, and be sure to request testimonials from the provider's current customer list.

Finally, when purchasing bandwidth, it is important to negotiate appropriate SLAs (Service LevelAgreements) with your providers. The SLA should state promised uptime and latency. It should also discuss rebates and remedies for failure to meet the agreed upon service levels.

5.12 Data Center Racks and Cabinets :

Figure 5.1 : Data Center Rack

All Data Centers are populated by some combination of racks, cabinets and enclosures. Racks and cabinets come in two widths – 483 mm (to accept ‘19 inch’ wide components) and 584 mm (to accept ‘23 inch’ wide components). Capacity is measured in Us, with 1U being 44.5 mm (1.75 in). Equipment intended for rack/cabinet installation is designed in multiples of Us (U1, U2, U3). Enclosure size is also given in Us (16U, 20U, etc.).

Enclosures should be both strong and rigid. Construction may be of aluminum (for weight considerations) and steel (for greater capacity and strength).

Racks Racks are open frames ready to be loaded with connection panels and/or active equipment. They can be floor-mounted or wall-mounted. Floor mounted racks are of either two or four post construction. Wall mounted versions usually have a swinging frontpiece to ease equipment access.

The traditional 7-foot floor mounted rack has a capacity of 45U. It could potentially hold up to 45 1U shelves, or 11 4U shelves or any combination of equipment and shelves that add up to 45U or less. Taller 8-foot racks are available that hold up to 52U.

Look for racks that offer horizontal and vertical cable management hardware options. Vertical cable management systems are essential for dependable network operation in that they keep cable organized, keep cables (especially fiber) from kinking and exceeding minimum bend radii and offer additional security.

Note that use of horizontal cable management will take up rack space the same way asshelves containing copper or fiber terminations. This should be carefully planned for when estimating the capacity of each rack.

The availability and placement of power strips is also an important consideration if theinstallation includes active equipment.

5.13 Wall Mount Enclosures

Wall mounted cabinets (also called enclosures, as in ‘telecommunications enclosure’) are fully encased, with front and rear doors for access to cables and equipment. Swing-out frames also help in that regard. They are vented for air circulation and may have fans for additional cooling.

5.14 Floor-Mounted Cabinets

Floor-mounted cabinets are fully enclosed units with metal sides and glass or metal front and rear doors. Cabinets are available to support 42U, 45U, or other capacities. Like racks, cabinets have rails that hold active equipment and shelves.Cabinets are designed to facilitate equipment cooling as much as they are for equipment containment and security. Since heat can degrade the performance of active electronics, cool airflow is an essential part of cabinet design. Cabinets are designed to act like chimneys. Cool air (or chilled air in larger equipment rooms and data centers) enters the cabinet from underneath the floor. As the active equipment heats the air, it rises and exits through the top of the cabinet. This creates a continuous circulation of cold air through the cabinet that cools the electronics. This natural convection can only draw away so much heat, so fans can be added at the top of the cabinet to increase airflow. With or without fans, it is important to limit the amount of air that enters or escapes at mid-height. Therefore, cabinet doors are usually solid.

Another common cooling method is to set up ‘hot and cold aisles.’ This is a scenario where cabinets are set up in rows with fronts facing fronts/backs facing backs so that vented cabinet doors allow cold air to be drawn through the front and pushed out the back. Modern datacenter systems recommends that the vented area be at least 60% open to allow unrestricted air flow.

5.15 Server cabinet :

Server cabinets Server cabinets are built to handle high densities of datacom active equipment and therefore support more weight. Additionally, server cabinets are typically deeper to accommodate the larger server equipment. Since there is no standard server depth, it can be difficult to accommodate more than one manufacturer’s servers within the same cabinet. However, server cabinets have vertical rails that can be adjusted to up to three different depths to handle multiple servers within the same cabinet.

5.16 Network cabinet:

Network cabinets are designed more for patch cord management. They have greater depth between the closed doors and rails to allow more room for patch cord organization.

6.17 Network Cabling:

To Design a modern data center, we must arrange network cabling as structured way. A structured cabling system is a complete system of cabling and associated hardware, which provides a comprehensive telecommunications infrastructure. This infrastructure serves a wide range of uses, such as to provide telephone service or transmit data through a computer network. It should not be device dependent.

The methods we use to complete and maintain cabling installations are relatively standard. The standardization of these installations is necessary because of the need to ensure acceptable system performance from increasingly complex arrangements.

Figure: Structured Cabling

5.18 The benefits of Structured cabling are:

- Consistency of design and installation;
- Conformance to physical and transmission line requirements;
- A basis for examining a proposed system expansion and other changes; and
- Uniform documentation.

5.19 Network Design:

We will design a hierarchical network for our modern data center. As compared to other network designs, a hierarchical network is easier to administrate and to expand, and problems can be solved more quickly.

A hierarchical network design subdivides the network into discrete layers. Each of these layers provides specific functions that define its role within the overall network. When the different functions provided in a network are made separate, the network design becomes modular and this also results in optimal scalability and performance.

5.20 Advantages of Hierarchical Networks

A number of advantages are associated with hierarchical network designs:

- Redundancy
  - Failover
  - Scalability
- Performance
- Security
- Ease of administration
- Maintainability

Since hierarchical networks are by nature scalable in an easy, modular fashion, they are also very maintainable. Maintenance for other network topologies becomes increasingly complicated as the network becomes larger. In addition, a fixed boundary for network growth exists for certain network design models, and if this boundary value is exceeded, maintenance becomes too complicated and too expensive. In the hierarchical design model, switching functions are defined for every layer, simplifying the selection of the

correct switch. This does not mean that adding switches to a layer does not lead to a bottleneck in another layer, or that some other restriction may occur. All switches in a fully meshed topology must be high-performance devices so the topology can achieve its

maximum performance. Every switch must be capable of performing all network functions. By contrast, switching functions in a hierarchical model are differentiated by layer. So in contrast to the Aggregation Layer and Core Layer, more cost-effective switches can be used in the Access Layer. Before designing the network, the diameter of the network must be first examined. Although a diameter is traditionally specified as a length value, in the case of network technology this parameter for the size of a network must be measured via the number of devices.

So network diameter refers to the number of devices that a data packet must pass in order to reach its recipient. Small networks can therefore ensure a lower, predictable latency

between devices. Latency refers to the time a network device requires to process a packet or a frame. Each switch in the network must specify the destination MAC address of the frame, look it up in its MAC address table and then forward the frame over the corresponding port. If an Ethernet frame must pass a number of switches, latencies add up even when the entire process only lasts a fraction of a second.

Very large volumes of data are generally transferred over “data center” switches, since these can handle communication for both server/server data as well as client/server data. For this reason, switches that are provided for data centers offer higher performance than those provided for terminal devices. Data centers are geared to tasks and requirements, which include mass storage in addition to arithmetic operations.

Networks for these data centers are high- and maximum-performance networks in which data transfer rates in the gigabit range can be achieved. Various high-speed technologies are therefore used in data center architectures, and data rates are increased using aggregation. Memory traffic (SAN) is handled over Fibre Channel (FC), client-server communication over Ethernet and server-server communication for example over InfiniBand. These different network concepts are being increasingly replaced by 10 gigabit Ethernet. The advantage of this technology is that a 40 Gbit/s version also exists, as well as 100 gigabit Ethernet. Therefore 40/100 gigabit Ethernet is also suited for the Core Layer and Aggregation Layer in data center architectures, and for the use of

ToR switches.

Chapter 6

Virtualization

6.1 Concept of Virtualization:

In a Modern Data center, server virtualization can reduce our costs on facilities, power, cooling, and hardware, simplify administration and maintenance.

Some benefits of server virtualization are:

- Save energy
- Save Space
- saving hardware cost
- Reduces downtime
- faster disaster recovery

6.1.1 Saving energy:

Migrating physical servers over to virtual machines and consolidating them onto far fewer physical servers means lowering monthly power and cooling costs in the data center. This was an early victory chant for server virtualization vendors.

Server virtualization allows business to encapsulate the operating systems and applications normally residing on individual servers into unique, software-based Virtual Machines (VMs), many of which can reside on a single server. This dramatically increases the portability, efficiency, manageability, reliability and end user accessibility of an organization's computing resources. It also dramatically lowers the energy consumption of a data center.

6.1.2 Saving floor space:

virtual server consolidation with virtualization will also reduce the overall footprint of our entire data center. That means far fewer servers, less networking gear, a smaller number of racks needed -- all of which translates into less data center floor space required.

Server virtualization offers a way to consolidate servers by allowing you to run multiple different workloads on one physical host server. A "virtual server" is a software implementation that executes programs like a real server. Multiple virtual servers can work simultaneously on one physical host server. Therefore, instead of operating many servers at low utilization, virtualization combines the processing power onto fewer servers that operate at higher total utilization in a single server.

6.1.3 Saving hardware cost :

As a general rule, business can expect up to a 10 to 1 reduction in the number of physical servers with a well planned and implemented virtualization project. By eliminating vast amounts of unused computing resources residing on underutilized servers and combining them onto virtualized environments, businesses can drastically reduce the number of servers in their data centers. While not always a bad thing, sometimes being tied down to one particular server vendor or even one particular server model can prove quite frustrating. But because server virtualization abstracts away the underlying hardware and replaces it with virtual hardware, data center managers and owners gain a lot more flexibility when it comes to the server equipment they can choose from. This can also be a handy negotiating tool with the hardware vendors when the time comes to renew or purchase more equipment.

6.1.4 Reduces downtime :

Most server virtualization platforms now offer a number of advanced features that just aren't found on physical servers, which helps with business continuity and increased uptime. Though the vendor feature names may be different, they usually offer capabilities such as live migration, storage migration, fault tolerance, high availability, and distributed resource scheduling. These technologies keep virtual machines chugging along or give them the ability to quickly recover from unplanned outages. The ability to quickly and easily move a virtual machine from one server to another is perhaps one of the greatest single benefits of virtualization with far-reaching uses. As the technology continues to mature to the point where it can do long-distance migrations, such as being able to move a virtual machine from one data center to another no matter the network latency involved, the virtual world will become that much more in demand.

6.1.5 Faster disaster recovery:

Virtualization offers an organization three important components when it comes to building out a disaster recovery solution. The first is its hardware abstraction capability. By removing the dependency on a particular hardware vendor or server model, a disaster recovery site no longer needs to keep identical hardware on hand to match the production environment, and IT can save money by buying cheaper hardware in the DR site since it rarely gets used. Second, by consolidating servers down to fewer physical machines in production, an organization can more easily create an affordable replication site. And third, most enterprise server virtualization platforms have software that can help automate the failover when a disaster does strike. The same software usually provides a way to test a disaster recovery failover as well. Imagine being able to actually test and see your failover plan work in reality, rather than hoping and praying that it will work if and when the time comes.

For Virtualization, we will use VMware as our virtualization server software.As virtualization is now a critical component to an overall IT strategy, it is important to choose the right vendor. VMware is the leading business virtualization infrastructure provider, offering the most trusted and reliable platform for building private clouds and federating to public clouds.VMware delivers on the core requirements for a data center virtualization infrastructure solution with very low cost. it is robust, reliable and easy to operate.

Chapter 7

Power Systems

7.1 Power :

Power is the one of the most important part of data center planning and design is to align the power and cooling requirements of the IT equipment with the capacity of infrastructure equipment to provide it.

7.2 PUE of Data Center:

Power usage effectiveness (**PUE**) is a measure of how efficiently a computer data center uses energy. Specifically, how much energy is used by the computing equipment (in contrast to cooling and other overhead).

PUE is the ratio of total amount of energy used by a computer data center facility to the energy delivered to computing equipment.

$$\mathrm{PUE} = \frac{\text{Total Facility Energy}}{\text{IT Equipment Energy}}$$

For modern data center, ideal PUE will be 1.0. Anything that isn't considered a computing device in a data center (i.e. lighting, cooling, etc.) falls into the category of facility energy consumption.

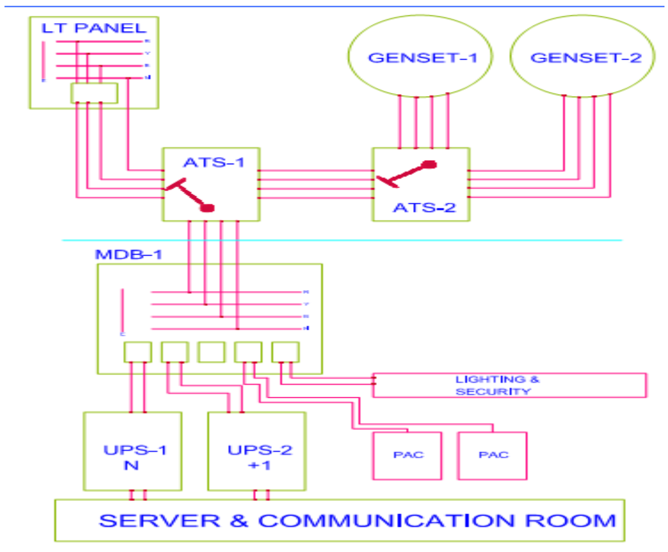

Figure 7.1 : Power Distribution Diagram

7.3 Power Density of Data Center:

The conventional method of specifying data center power density in (538 W /m 2). provides very energy efficiency for critical questions that are faced by data center operators today. In particular, the historical power density specification does not meet our modern concept of data center. This is a very practical ,because the modern data center today has a density rating of 1.5 kW per rack while typical IT equipment has a greater power density of 3-20 kW per rack when use Tower Server. It is possible because we will use blade server for better power and density efficiency.

7.4 Power Supply:

Planning power for our data center normally requires planning these four components of a power plan:

• Electrical power from the local utility company

• Power filtering and monitoring

• UPSs (Uninterruptible Power Supplies)

• Backup Generators

The main planning task involving electrical power from the local utility company concerns power grids. It is best if your data center can be connected to multiple power grids. If power to one grid is lost, all or at least some portion of our data center will continue to operate normally. Bear in mind that multiple power grids will require multiple sets of power transformers, circuit breaker panels, and battery backup units.

Power requirements can be determined by researching manufacturer specifications for each piece of equipment you wish to place in our data center and tallying the results. However, the average lifespan for a server is four years and hopefully our data center will survive many iterations of new server technology. Therefore, we have to plan with generous rough estimates and add a safety factor (20-50%) for growth.

Keep in mind that if the devices have redundant power supplies, you must figure in the combined wattage drain.A current industry standard for estimating power requirements is to estimate 60 watts of power per spare foot. As network and server devices are becoming smaller and smaller, the standard estimation is quickly rising to 100 watts per square foot. Another equation that yields similar, but not identical, results is to estimate 4 kilowatts of power per 19” rack. Just a few years ago, that rule of thumb was 2 kilowatts per 19” rack.

When calculating the total power requirement to feed your data center, you must figure in the power required by the HVAC system.

A standard way to measure this is to add up the total equipment power requirement and add 70 percent. Power typically needs to be available in both 115v and 230v to every location within the data center. The proper jacks must be installed to match the type the equipment you will be connecting. You must also determine if your equipment will need single or three phase power. Some equipment will require special adapters for connection to single or three-phase power; ensure that you have reviewed the technical specifications for any device that does not plug into a standard 110VAC 60 cycle receptacle. Power to devices with redundant power supplies should come from separate circuits, providing an additional layer of redundancy and stability.

7.5 Power distribution unit:

Figure 7.2 : power distribution unit

A **power distribution unit** (**PDU**) or **mains distribution unit** (**MDU**) is a device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment located within the data center.[1] Each PDU power inlet is fused for surge protection and power fluctuations. We will use APC PDU for our data center.

7.6 Power backup systems:

7.6.1 UPS :

UPS sizing should take into account the amount of total power required to operate the data center and the length of time required to get the backup generator into service.

Generator sizing should take into account the total power required to operate the data center and the total length of time you want the data center to be able to operate on its own power. It does little good for your generator to provide 2,000amps if it runs out of fuel in 30 minutes. Make sure you include the HVAC and emergency lighting power requirements in your calculations. UPS capacity is typically measured in Volt-Amp's (VA). VA is a unit for measuring power. Like the Watt (W), it describes a quantity of electrical power. To convert from W to VA, multiply by 1.4.

To convert from VA to W, multiply by 0.714. Make sure you size the UPS with your equipment's peak power load in mind. A device might draw 1000 watts during normal operation but when the device is turned on it might draw 1500 for startup. You must size a UPS that will handle this peak load.

Both UPSs and backup generators should be tested at regular intervals, at least once every six months. Depending upon your business requirements, redundant UPS may be appropriate. In our Data Center we will use two APC Matrix- XR UPS 5KVA systems for our server.

7.6.2 Backup Generators:

A backup or **standby generator** is a back-up electrical system that operates automatically. Within seconds of a utility outage an automatic transfer switch senses the power loss, commands the generator to start and then transfers the electrical load to the generator. The standby generator begins supplying power to the circuits. After utility power returns, the automatic transfer switch transfers the electrical load back to the utility and signals the standby generator to shut off. It then returns to standby mode where it awaits the next outage. To ensure a proper response to an outage, a standby generator runs weekly self-tests. Most units run on diesel, natural gas ,patrol etc.

Automatic standby generator systems may be required by building codes for critical safety systems Modern data center's power supply.

7.7 Power Conditioners:

The electronic equipment that the data center will house can be extremely sensitive to “dirty "power. “Dirty” power is that which has high frequency noise in the line, varying voltages, surges, and other electrical impurities. These electrical impurities can disrupt and even ruin sensitive electronic equipment. The electrical system should be tested for quality of power. If not found to be within acceptable tolerances, power conditioners can be installed to “clean” the power and protect the data center equipment.

7.8 Surge Arrestors:

Voltage spikes can disrupt or even destroy data center equipment. Surge arresting equipment should be included as part of the electrical system. Most Power conditioners and UPSs perform surge arresting as part of their feature set. If you are not using a power conditioner or UPS, a separate surge arresting unit must be installed.

Chapter 8

Data Center Cooling

8.1 Cooling Systems :

To satisfy the mission critical installation cooling challenges identified in this study, there are a number of changes required from current design practice. Many of these changes will require changes in the technology and design of cooling equipment, and how it is specified. Integration of the components of the cooling subsystem, particularly the air distribution and return systems, must move away from the current practice of unique system designs, and toward pre-engineered and even pre-manufactured solutions. Such solutions would ideally be modular and standardized, expandable at will, and would ship complete but in parts that would rapidly plug together on site. Standardization will facilitate the learning process.

As electricity prices and IT power consumption continue to rise, IT-related energy costs are getting increased scrutiny. Cooling systems taking approximately 37 percent of electricity usage within a well-designed data center and, in many cases, represents a significant opportunity to reduce IT energy costs.

We figure out that the following five strategies will help to increasing data center cooling efficiency:

1. Proper sealing of the data center environment:A vapor seal plays a critical role in controlling relative humidity, reducing unnecessaryhumidification and dehumidification.

2. Optimizing air flow:Rack arrangement, computer room air conditioner placement and cable managementall impact the amount of energy expended to move air within the critical facility.

3. Using thermostat where appropriate:Thermostat system control room temperature to be used to support data center systems, when temperature goes down then level, it will stop the cooler and when temperature going high it will start the cooler and creating opportunities for energy saving cooling systems.

4. Increasing cooling system efficiency:

New technologies, such as variable capacity systems and improved controls, are drivingincreased efficiency of room air conditioning systems.

5. Bringing cooling closer to the source of heatSupplemental cooling systems bring cooling closer to the source of heat, reducing theamount of energy required for air movement.

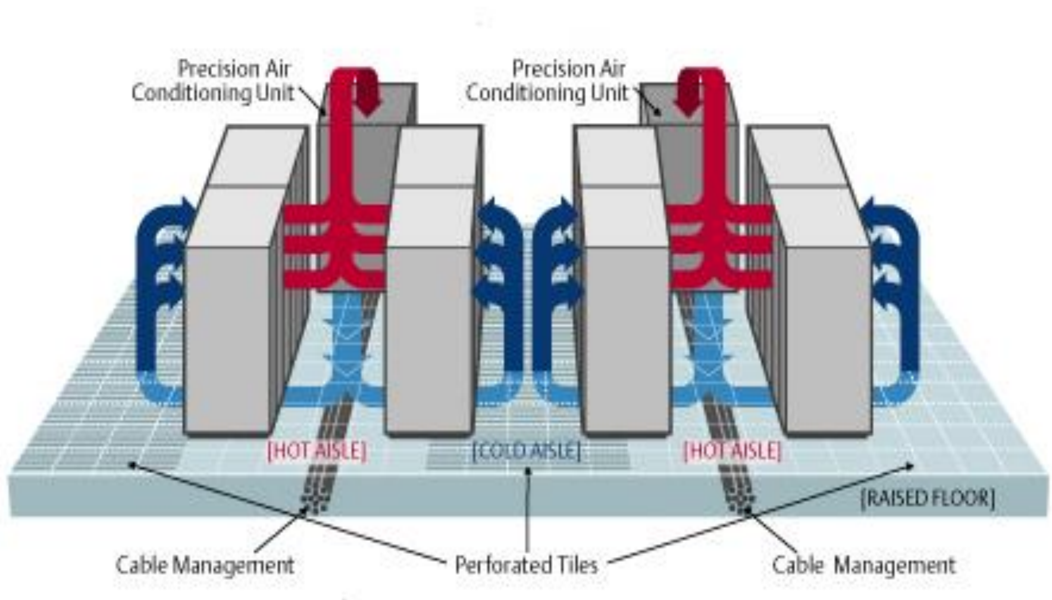

Figure 8.1 : Data Center Cooling systems by Precision A/C .

Considering above features, we will use two precision air-conditioning systems to fulfill our requirements. Together, these methods can reduce cooling system energy costs by 30 to 45 percent and generate significant, recurring savings. Coupled with emerging technologies such ashigher-efficiency processors and new chip-based cooling technologies, these measurescan keep energy costs in line as server densities and the price of energy continue to rise.

Chapter 9

Security

9.1 Data center security:

The data center not only contains very expensive equipment that someone might want to steal,but also valuable data that essential to our organizations survival. We must make sure that the data center is protected against theft, sabotage, vandalism, and industrial espionage. For that purpose, overall security policies should be put in place that address all issues in a high level fashion, defining guidelines for the more specific physical, computer and network security requirements.

Data center needs two types of Securty.they are ,

1.Physical Security

2.Logical Security

The key item to remember, especially in regards to computer and networksecurity, is that nothing is foolproof.

9.2 Physical Security

The NOC can also function as the point of security control for the data center. If you allow access to the data center only through the NOC, you have a single point for monitoring and control.

There are several things to keep in mind when designing physical security into a data center.

9.2.1 Data Center Security Staff

These individuals should perform a host of duties on a daily basis, such as monitor intrusion security alarm systems; dispatch mobile security officers to emergencies; monitoring to prevent unauthorized access, such as tailgating; assist all individuals who have authorized access to enter the data center; controlling access to the data center by confirming identity; issue and retrieve access badges; respond to telephone and radio communications..

9.2.2 Electronic Access Control Systems (ACS)

Access to all entry points into and within the data center should be protected by electronic access control mechanisms which allow only authorized individuals to enter the facility. Included within the framework of electronic access control should also be biometric safeguards, such as palm readers, iris recognition, and fingerprint readers.

Figure 9.1 : Electronic Access Control

9.2.3 **Provisioning Process**

Any individual requesting access to the data center should be enrolled in a structured and documented provisioning process for ensuring the integrity of the person entering the facility.

9.2.4 **Visitors**

All visitors must be properly identified with a current, valid form of identification and must be given a temporary facility badge allowing access to certain areas within the data center. This process must be documented in a ticketing system also.

9.2.5Alarms & Motion Detector:

All exterior doors and sensitive areas within the facility must be hard wired with automatic alarms. alarms and Motion detectors should be employed and monitored. Deployment underraised flooring and in drop ceilings not only helps detect unauthorized intrusion, but canhelp maintain a stable environment by detecting, and preventing, unscheduled (and unauthorized) maintenance to take place to cable runs, power, or other critical systems.

9.2.6Surveillance Cameras

Surveillance cameras should be installed around the perimeter of the building, at all entrances and exits, and at every access point throughout the building. A combination of motion-detection devices, low-light cameras, pan-tilt-zoom (PTZ) cameras and standard fixed cameras is ideal. Footage should be digitally recorded and stored offsite.

Figure 9.2 : Surveillance Cameras

The facility should have a mixture of security cameras in place throughout all critical areas, both inside and out, of the data center. This should include the following cameras: Fixed and pan, tilt, and zoom (PTZ) cameras.

9.2.7Badge and Equipment Checks

Periodic checks should be done on employees and customers regarding badge access and equipment ownership.

9.2.8Local Law Enforcement Agencies

Management should have documented contact information for all local law enforcement officials in the case of an emergency.

9.3 Logical Security

Protecting data through logical means – firewalls, anti-malware programs, etc. – is just as important as physical security.Logical security often call cyber security.There are few issues are to be consider to designing Logical security into a data center. They are ,

29.3.1Computer Security

• Several levels of authorization should exist for administering devices. Engineers shouldbe granted the minimum access necessary to complete their tasks.

• Server console access should be exclusive to a separate administrative network that canonly be accessed from the NOC, where possible. If requirements specify access from acentral administration area outside of the NOC, network connectivity should be run to that specific location, parallel to the company's internal backbone. At the very least, strong encryption should be used for this kind of access.

9.3.2Network Security

Network security is best implemented in a tiered fashion.

• Tier 1 is typically edge-access protection via firewalls for safeguarding access intothe network.

• Tier 2 may be a firewall that separates publicly accessible devices such as webservers, DNS servers, mail relays, etc. from the rest of the internal network. Manytimes the Tier 1 and Tier 2 policies reside on the same physical device. In addition,communications that pass confidential or sensitive data to the outside should bestrongly encrypted using a method like VPN tunneling that can be setup in parallel tothe firewall.

• Tier 3 may also be implemented in environments where highly critical information,databases, or other such assets require additional separation from the rest of thenetwork. We will use cisco asa 5525X as our firewall for our data center

9.3.3 Intrusion Detection & Prevention systems

No matter how strong the security is compromises and incidents could occur. It is therefore very important to have a means of detecting such a breach in order to be able to respond to it and handle it in an appropriate manner. This should be implemented and available on both thecomputer and network level.an IDP & IPS is built-in in our cisco asa 5525X firewall for our data center

Chapter 10

Fire Detection and Suppression

10.1 fire detection

With the value of data center being extraordinarily high, down time is not an option. Servers other electrical equipments are packed together, the power is always on, they generate heat, and while not widely publicized, they do catch fire. Should any fire occur?? it is most important, after securing the safety of personnel, to ensure that equipment suffers a minimum of damage. The datacenter fire detection and protection requirement is to put out the fire and get datacenter back up and running within hours.

From our study, we found following components for modern datacenter friendly include:

1. Fire Detection systems
2. Automatic fire suppression systems
3. Emergency power off Switch

10.1.1 Fire detection: A fire detection system that detects smoke or fire and make alarm that includes both a loud noise and flashing lights automatically .This systems must be used at ceiling level or under raised floor.

10.1.2 Automatic fire suppression systems : An automatic fire suppression systems control and extinguish fires automatically and without human intervention. Today there are numerous types of Automatic Fire Suppression Systems. Systems are as diverse as the many applications. But we must careful about any water based Fire Suppression Systems as data center use various electrical and electronic devices.

Figure 10.1: FM-200 fire suppression system.

We will use gas based agent like FM-200 Agent in automatic fire suppression systems. FM200 is the best option for fire suppression. FM200 employs heptafluoropropane, an invisible gas that draws the heat energy out of the fire and stops combustion.

It is not damaging to the equipment or personnel. With the use of this non-harmful agent, the data center can return to operation more quickly after a fire incident. When using a gas suppression system, the law requires that manual abort switches be placed in easily accessible locations throughout the center.

10.3 Emergency power off Switch:

Emergency Power Off switchsystem is a safety feature intended to power down of information technology equipments, a data center or an entire facility in an emergency such as fire, flood and HVAC failure resulting in overheating of sensitive equipment - thus protecting the facility and personnel automatically.

Figure 10.2 : Emergency Power off (EPO) Switch.

From these systems we will get following benefits,

- De-energize equipment during any fire
- Close fire dampers and turn off ventilation and cooling equipment to contain fire and maintain proper concentration of fire suppressant
- Safely shutdown equipment during a flood or sprinkler system discharge
- Help protect fire department personnel from electrocution when fighting a fire

Chapter 11

DISASTER RECOVERY

11.1 Concept of disaster recovery:

Disaster recovery is the area of security planning that deals with protecting an organization from the effects of significant negative events. Significant negative events, in this context, can include anything that puts an organization's operations at risk: crippling cyber attacks and equipment failures, for example, as well as hurricanes, earthquakes and other natural disasters.

With proper planning, we can minimize the impact that a disaster can have on our data Center operation.

11.2 Data Backups :

Tape backups are the most common and least expensive form of backup today. Backups are usually run daily with the tapes being kept offsite for safe storage. This not only protects you from losing the data if the data center is destroyed, but also protects against accidental erasure or

corruption on the main storage hard drive. Data vaulting is another method of data backup which involve a WAN link to a remote backup facility. The data is continuously backed up across the wire and archived off site. This allows you to have up to the minute off site backups compared to the usual daily backups with a tape storage scheme. It also allows for immediate access to your backed up data, should you need it. This method is substantially more expensive than tape backup, so determine your requirements andplan accordingly.

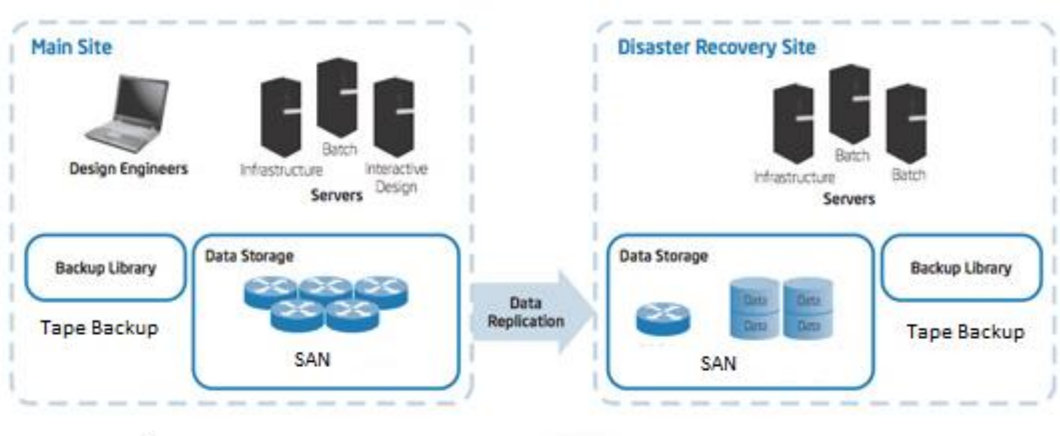

Figure 11.1: Disaster recovery System

In Our Data Center we will take following strategies for data protection include:

- Data Backups made to tape and sent off-site at regular intervals
- Data Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk

replication of data to an off-site location, which overcomes the need to restore the data by use of storage area network (SAN) technology.

Chapter 12

Data Center Monitoring

12.1 Data Center Monitoring concept:

To get a full view of the data center environment including servers,services,virtualized environments, UPS, power, HVAC, Security, Uptime etc, we need a strong monitoring systems.

Our Data center monitoring system is a comprehensive data center monitoring and server monitoring software solution for modern environments that include a complex mix of IT infrastructure and applications based on next-generation technologies, such as Virtualization, Cloud Computing and Grid Architectures. it also monitors a variety of power and environmental equipment and infrastructure, such as, HVAC, UPS and Generators, in addition to its proven support for all IT infrastructure. Traverse is a data-agnostic and extensible platform that can monitor any data center component.

Data center complexity, dynamic cloud resources, and the increasing demand for IT service assurance requires a new way to manage the data center using an integrated and service-oriented approach. The ever evolving technology and increasing business challenges like virtualization, server and data center consolidation require a robust server monitoring solution that includes monitoring of virtual resources. A server management solution that is proactive and up-to-date with changing technologies is an intelligent way to manage your business efficiently.

Figure: Data Center Monitoring

12.2 Advantages of monitoring systems:

Advantages of effective server monitoring include:

- Monitoring performance of our servers 24/7
- Troubleshooting and resolution of system bottlenecks
- Monitoring key data center services
- Securing servers against internal and external threats
- Analyzing server usage trends for optimal capacity planning
- Report generation
- Monitoring power and cooling and other systems

In our Modern data Center, We will use Kaseya Traverse Software as our data center monitoring systems. Kaseya Traverse utilize the industry's leading cloud and service level management platform. Designed to work across cloud, on-premise, hybrid cloud, virtualized and distributed IT environments, Kaseya Traverse provides central command and remote monitoring of the IT infrastructure enabling the vital business services you support. Using powerful instrumentation and automation, Kaseya Traverse's root-cause analysis capabilities enable you to get to the bottom of complex problems quickly and easily manage service level agreements (SLAs) via predictive analytics and smart, contextual monitoring.

Chapter 13

Case Study

Now we will describe the equipments that needed to design our modern data center. By this presentation we will make a Tier -ii type standalone Data Center for a Medium Organization or Institute.

Our necessary equipments descriptions are like follows,

Data Center Electrical Works

SL#	Specification	Unit
1	**NYY- 4X70sm** Insulated PVC sheathed 4 core cable rated voltage 600/1000V, Permissible Voltage 720/1200 Fixed: -15°C to +70°C for cable through Ladder. low copper loss and BDS standard. From Control Room to MDB.	Meter
2	**NYY- 4X16rm** Insulated PVC sheathed 4 core cable rated voltage 600/1000V, Permissible Voltage 600/1000 Fixed: 15ºC to 35ºC for cable through Cable Ladder Which low copper loss and BDS standard. From MDB to UPS-1&2 input & output wiring.	Meter
3	**NYY- 4X6rm** Insulated PVC sheathed 4 core cable rated voltage 600/1000V, Permissible Voltage 600/1000 Fixed: 15ºC to 35ºC for cable throughCable Ladder which low copper loss and BDS standard. From MDB to Precission Aircondition.	Meter
4	**NYY- 3X4rm** Insulated PVC sheathed 3 core cable rated voltage 600/1000V, Permissible Voltage 300/500 Fixed: 15ºC to 35ºC for cable through Cable Ladder which low copper loss and BDS standard. From UPS output SDB to Industrial Socket.	Meter
5	**NYY- 3X2.5rm** Insulated PVC sheathed 3 core cable rated voltage 600/1000V, Permissible Voltage 300/500 Fixed: 15ºC to 35ºC for cable through Cable Ladder which low copper loss and BDS standard. From UPS output SDB to Auxiliary Socket.	Meter

6	**IYAL 1.3rm** PVC Insulated Non-Sheathed Single Core Cable (250/440 V) 3/0.029 cable through Aluminium Channel For Lighting Wiring	Meter
7	**INDUSTRIAL SOCKET:** 3-Pin socket with 3-Plug earthling point , 220v~250v AC, Maximum Current 40Amps Operating Temperature: <-5ºc~55ºc>,with protected cover and gripper.	No.
8	**AUXILIARY SOCKET:** 3-Pin socket with earthling point , 220v~250v AC, Maximum Current 15Amps Operating Temperature: <-5ºc~55ºc>,made of fire proof materials with PVC MK box.	No.
9	**Ceiling Mounted Energy Saving Light: PL LIGHT SET**.	No.
	Dimention:162x140x135mm main body	No.
	Dimention:245x80x11mm Extension pipe	No.
	Hanging length:425mm (Aprox)	No.
	Base: 78X78mm to installation Alluminium Channel	No.
	Colour: Black	

Grounding / Earthing System:

Sl#	**Specification**	**Unit**
1	**Inside the earth with (150 feetX2) Boring**	
	Copper Wire (Size: 02 SWG)	Meter
	Copper Rod	Meter
	G.I. Pipe (1.5”) diameter	Meter
2	**From the ground to Equipment room through PVC pipe**	
	Cable Size **35 rm NYY** (Green Insulation)Brand: **Eastern**. Origin: **Bangladesh**.	Meter

	PVC pipe: 1 inch diameter	Mete r
	Saddle: 1 inch	No.
	Royal Plug	Box
	Wooden Screw	Box
	Copper Bar & Clamp 12inch X 1.25inch X 3mm bar with clamp	No.
3	**Equipment Room cabling**	
	G.N.D Bus-bar (Long)	No.
	G.N.D Bus-bar (Small)	No.
	Cable BYA2.5 re (Green)	Mete r
	Cable Lux (Copper)	No.
	Other Accessories	Lot

Fire Protection, CCTV and BMS

Sl#	**Specification**	**Unit**
1	Cabling c/w PVC Conduit for Access Control System (CAT 6, 3 Core Power Cable)	Lot
2	Testing Installation and Commissioning of Access Control System	Lot
3	Cabling c/w PVC Conduit for CCTV System (RJ58\RJ59 and 1.5rm)	Lot
4	Cabling c/w PVC Conduit for Environment Monitoring System (2 Pair Cable, 3 Core Power Cable)	Lot
5	Water Detection Cable	Meter
6	40 MS Pipe for FM200 Gas Suppression System	Lot

Electronic Access Control

Sl#	Items	Unit
1	TCP/IP based door Access Controller	1
2	MIFARE Smart Card Reader	4
3	MIFARE Smart Card	50
4	Keypad	2
5	Magnetic Door Sensor	2
6	Electric Magnetic Lock, 600 lbs	2
7	Power Supply Unit c/w 12 Vdc, 7 AH battery back up	1
8	U-channel/ZL Bracket	2
9	Emergency Lock Release Key	2
10	Access Management Software with 16 door license	1
11	2 Hours Rated Fire Resisting Door with Fire Resistant Vision Panel	2

Raised Floor, UPS, Generetor, Air Conditioning & Environment Monitoring System

Sl#	**Items**	**Unit**
1	Raised Access Floor	1
2	UPS for Data Center	2
3	UPS for IT equipment at the user end	2

4	Precision AC	2
5	Redundant Generator 33 KVA FG Wilson	1

Environment Monitoring System

5	Network based BAS Controller	Trend	1
6	16 Digital Input Expansion Board	16 Digital Inputs	1
7	Space Temperature and Humidity Sensor		1
8	Air Quality Sensor		1
9	Single Relay Module Card		2
10	GSM Module		1
11	Environment Monitoring Software		1

Data Centre Equipment (FM200 Fire Protection System)

Sl#	Items	Description	Unit
1	550 Lbs Cylinder with Primary Completer Kit	Chemetron, Gamma 550 lbs	1
2	FM200 Gas	FM200 Gas	139
3	Control Panel	Notifier RP1200	1
4	Optical Smoke Detector	Hochiki SLV	8
5	Gas Dischrge Nozzle (32 mm)	32 mm	2

6	Gas Dischrge Nozzle (20 mm)	20 mm	2
7	Alarm Bell	Kobishi MBA	1
8	Horn with Flash Light	System Sensor P2xxx	1
9	Manual Gas Release Switch	KAC WY2xxx	1
10	Manual Abort Switch	KAC WY9xxx	1
11	"Evacuate Area" Sign	Sign	1
12	Front Strap	Front Strap	1
13	Fire Resistant Cable	Eastern BYA-FR 1.3 mm	1000

Data Centre Equipment (CCTV)

Sl#	Items	Description	Unit
1	4 Channel DVR Server with 750 GB HDD		1
2	High Resolution IR Colour Dome Camera c/w PSU		4
3	Single Site Video Monitoring Software		1
4	19" Colour LCD Monitor		1

Blade Server :

Sl#	Items	Unit
1	Dell blade server R710	4

Server racks & Cabinets

Sl#	**Items**	**Unit**
1	42 U Rack(78.74 X 23.62 X 31.50 inch)	4
2	9 U Cabinet **(** Built-In Fan Locking Lock & Key)	2
3	Cable Manager	2

Fire wall:

Sl#	Items	Unit
1	Cisco Asa 5525X	2

Network Switch:

Sl#	Items	Unit
1	Cisco 3750 XL Switch	2
2	Cisco 3560 Tcl Switch	2
3	Cisco 2960 TCS Switch	4

Chapter 14

Conclusion

With considering the above issues and in order to support the demanding availability requirements of today's applications, modern data centers need to go beyond the redundancy requirements of yesteryears to a more future-proofed resilient infrastructure that will serve them well down the road. This requires organizations to support modern technologies and standards, and also choose a solution that will provide an open and flexible enough architecture to support the evolving needs of the upcoming business. During the internship I have been trained by professionals to observe and learn the designing, maintenance and security management of amodern data center that improves application performance and increases business agility, providing customers with a future-proofed approach to data center design best practices.

References:

- ✓ http://en.wikipedia.org/wiki/Datacenter
- ✓ http://www.datacenterknowledge.com/archives/2010/10/13/choosing-a-data-center-cooling-system/
- ✓ http://www. uptimeinstitute.com/publications
- ✓ http://www-935.ibm.com/services/us/en/it-services/data-center/site-and-facilities-services/index.html
- ✓ http://www.dell.com/learn/us/en/19/software-data-center-cloud-management-virtualization
- ✓ http://www.cisco.com/c/en/us/solutions/data-center-virtualization/solution-listing.html
- ✓ http://en.wikibooks.org/wiki/The_Design_and_Organization_of_Data_Centers
- ✓ Data Center Technology Design Guide -by Cisco
- ✓ Administering Data Centers - by Kailash Jayaswal
- ✓ http://www.hightech.lbl.gov/documents/data_centers/06_datacenters-pge.pdf

- ✓ http://www.belden.com/pdfs/techbull/datacenterguide.pdf
- ✓ www.commscope.com
- ✓ www.commscope.com/docs/data_center_design_guide.pdf
- ✓ RDM Data Center Handbook
- ✓ http://www.kaseya.com/solutions/