Data Center Design Criteria

Course Content

Module 1

- Data Center Layers
- Data Center Feasibility Studies and Project Cost Budgeting
- Risk Assessment
- Power and Cooling Systems Analysis
- Business Continuity and Disaster Recovery
- Data Center Site Selection

Module 2

- Type of Server Farms in Data Center
- Server Farm Topologies and Network Infrastructure in Data Center
- Cable Management

Module 3

- Electrical Power & Cooling requirement
- UPS and Battery systems
- Generator and Automatic transfer switch equipment
- Fire Alarm System and Sprinkler systems
- Security

Module 1

Data Center Layers

The data center design process starts by working with the management staff to determine business's data center project needs and combine this with the understanding of the trends and migration strategies required in adapting to future changes. Finally a conceptual data center design is developed and from which construction budget and time lines are put together.

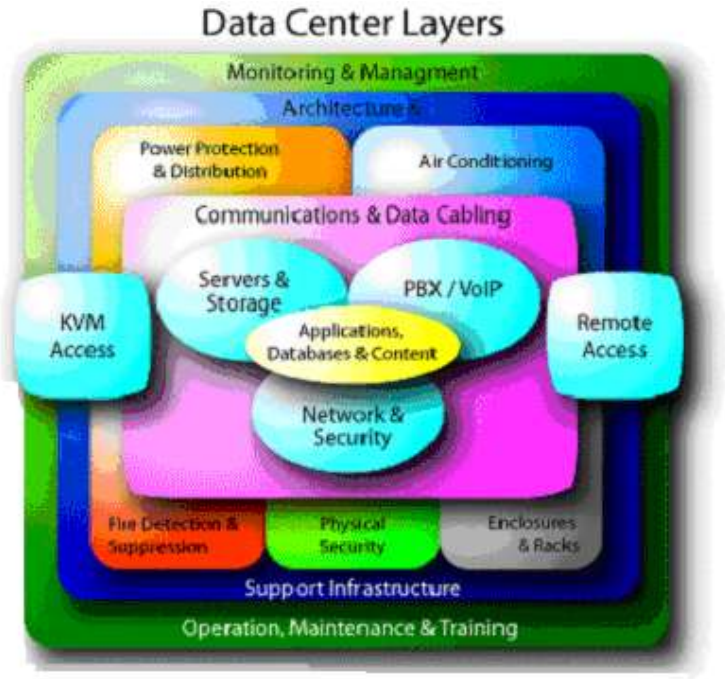

Figure 1-1: Data Center Layers

The modern Data center has various components. Figure 1.1 above shows all the components as different layers. All the layers will be discussed in detail in this course.

As shown graphically in this figure, "Applications, Database & Content" layer is the core layer which is the prime concern for corporation's user's point of view. But as we can see from the figure 1.1, for reliability and accessibility of this "core" layer there are several other layers need to be designed properly for Data center to be ideal.

Three important attributes of any good Data Center Design are ***scalability, flexibility and high availability.***

Scalability:
The Data Center Design must support fast and seamless growth without major disruptions.

Flexibility:
The Data Center Design must support new services without a major overhaul of its infrastructure.

High Availability:
The Data Center Design must minimize single point of failure and offer predictable uptime by incorporating concurrent maintainability and fault-tolerance against hard failures.

Data Center Feasibility Studies and Project Cost:

Data center project feasibility and cost budgeting is accomplished by applying Key Design Criteria of the two main categories of the budget:

- **The Information Technology Infrastructure & Services (IT):**

Each corporation has different Infrastructure in place depending upon the nature of the business. Spacing, Engineering and Security design depends a lot on primary use of the Data Center.

Infrastructure can be mix of various manufacturers for the same type of equipment, for example, Data servers can be from manufactures like Sun, IBM, Dell or Compaq. This prompts for different Rack types and different power outlet requirement for each type of servers.

It is important to know the migration schedule from IT department of existing hardware for Flexibility.

- **Support Infrastructure and Services (Facility):**

Location and size of the data center should be well coordinated with IT staff and facility maintenance staff.

Electrical and Air Conditioning: while selecting a location and space, Electrical and Air conditioning must be kept in mind. It should be feasible to add extra electrical and Air conditioning loads.
Maintenance staff: dedicated and trained maintenance staff should be available 24x7 to support data center issues.

Risk Assessment:

A comprehensive data center inspection is needed to assess the ability of the support infrastructure to provide continuous availability which include the following:

- An evaluation of the present load condition
- A comparison to the capacity constraints
- Identification of critical deficiencies
- Potential downtime risks
- An assessment of the concurrent maintenance capacity of the site

Power and Cooling Systems Analysis:

A complete load profiling and reporting from simple spot-checking to week-long data should be used to accomplish the following:

- An evaluation of the present load condition
- A comparison to the capacity constraints
- Identification of critical deficiencies
- An assessment of the concurrent maintenance capacity of the site
- Redundant power supplies, 24 x7 backup facilities, multiple environment control systems

Business Continuity and Disaster Recovery:

A detailed assessment must be made while designing a data center for the following:

Identify Mission Critical Applications and Servers
Staff availability in the event of Disaster
Remote access to Applications

Site Selection:

Data Center Site selection should be made based on all the above discussed factors.

Module 2

Types of Server Farms and Data Centers

As depicted in Figure 2-1, three distinct types of server farms exist:

- Internet
- Extranet
- Intranet

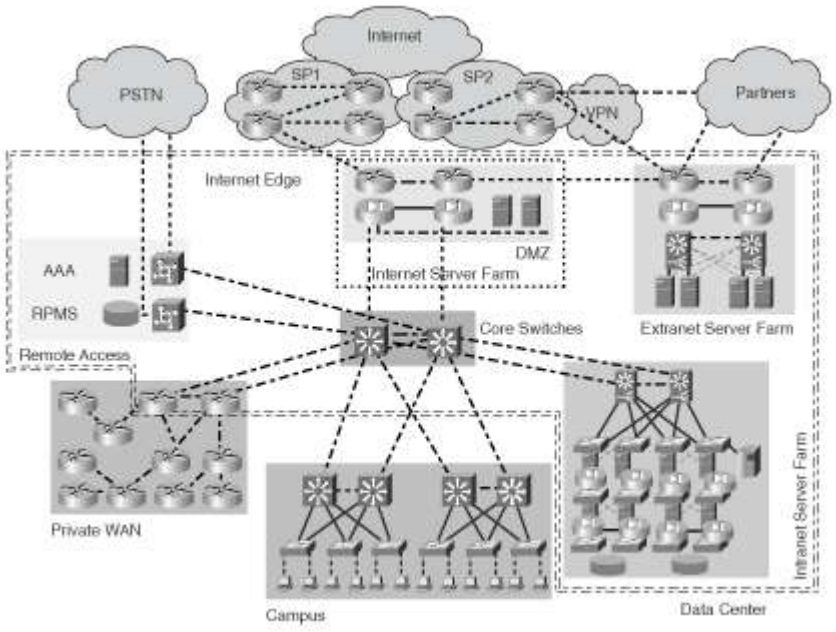

Figure 2-1 Overview of Data center Topology

All three types reside in a Data Center and often in the same Data Center facility, which generally is referred to as the *corporate Data Center* or *enterprise Data Center*. If the sole purpose of the Data Center is to support Internet-facing applications and server farms, the Data Center is referred to as an *Internet Data Center*.

Server farms are at the heart of the Data Center. In fact, Data Centers are built to support at least one type of server farm. Although different types of server farms share many architectural requirements, their objectives differ. Thus, the particular set of Data Center requirements depends on which type of server farm must be supported. Each type of server farm has a distinct set of infrastructure, security, and management requirements that must be addressed in the design of the server farm. Although each server farm design

and its specific topology might be different, the design guidelines apply equally to them all. The following sections introduce server farms.

Internet Server Farms

As their name indicates, Internet server farms face the Internet. This implies that users accessing the server farms primarily are located somewhere on the Internet and use the Internet to reach the server farm. Internet server farms are then available to the Internet community at large and support business-to-consumer services. Typically, internal users also have access to the Internet server farms. The server farm services and their users rely on the use of web interfaces and web browsers, which makes them pervasive on Internet environments.

Two distinct types of Internet server farms exist. The dedicated Internet server farm, shown in Figure 2-2, is built to support large-scale Internet-facing applications that support the core business function. Typically, the core business function is based on an Internet presence or Internet commerce.

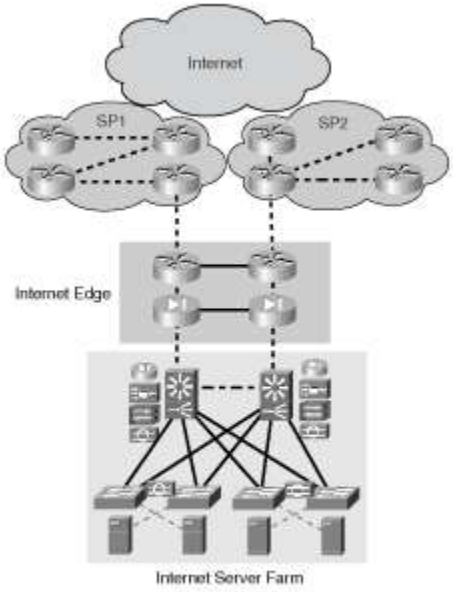

Figure 2-2 Dedicated Internet Server Farms

In general, dedicated Internet server farms exist to sustain the enterprise's e-business goals. Security and scalability are a major concern in this type of server farm. On one hand, most users accessing the server farm are located on the Internet, thereby introducing higher security risks; on the other hand, the number of likely users is very high, which could easily cause scalability problems.

The Data Center that supports this type of server farm is often referred to as an Internet Data Center (IDC). IDCs are built both by enterprises to support their own e-business infrastructure and by service providers selling hosting services, thus allowing enterprises to collocate the e-business infrastructure in the provider's network.

Intranet Server Farms

The evolution of the client/server model and the wide adoption of web-based applications on the Internet was the foundation for building intranets. Intranet server farms resemble the Internet server farms in their ease of access, yet they are available only to the enterprise's internal users. As described earlier in this chapter, intranet server farms include most of the enterprise-critical computing resources that support business processes and internal applications. This list of critical resources includes midrange and mainframe systems that support a wide variety of applications. Figure 2-3 illustrates the intranet server farm.

Notice that the intranet server farm module is connected to the core switches that form a portion of the enterprise backbone and provide connectivity between the private WAN and Internet Edge modules. The users accessing the intranet server farm are located in the campus and private WAN. Internet users typically are not permitted access to the intranet; however, internal users using the Internet as transport have access to the intranet using virtual private network (VPN) technology.

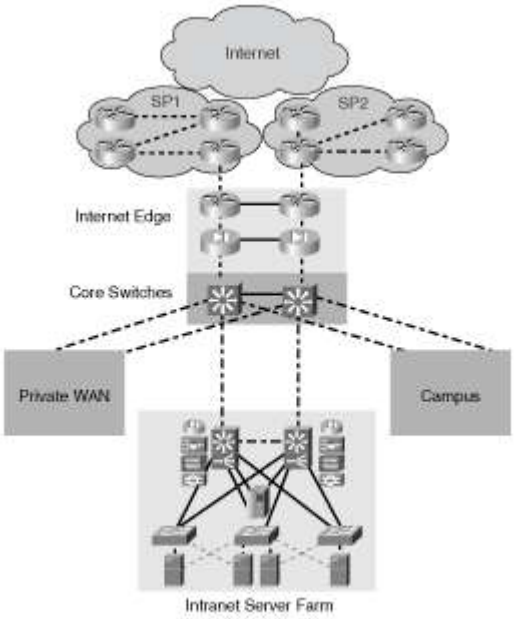

Figure 2-3: Intranet Server Farms

The Internet Edge module supports several functions that include the following:

- Securing the enterprise network
- Controlling Internet access from the intranet
- Controlling access to the Internet server farms

The Data Center provides additional security to further protect the data in the intranet server farm. This is accomplished by applying the security policies to the edge of the Data Center as well as to the applicable application tiers when attempting to harden communication between servers on different tiers. The security design applied to each tier depends on the architecture of the applications and the desired security level.

Extranet Server Farms

From a functional perspective, extranet server farms sit between Internet and intranet server farms. Extranet server farms continue the trend of using web-based applications, but, unlike Internet- or intranet-based server farms, they are accessed only by a selected group of users that are neither Internet- nor intranet-based. Extranet server farms are mainly available to business partners that are considered external yet trusted users. The main purpose for extranets is to improve business-to-business communication by allowing faster exchange of information in a user-friendly and secure environment. This reduces time to market and the cost of conducting business. The communication between the enterprise and its business partners, traditionally supported by dedicated links, rapidly is being migrated to a VPN infrastructure because of the ease of the setup, lower costs, and the support for concurrent voice, video, and data traffic over an IP network.

Many factors must be considered in the design of the extranet topology, including scalability, availability, and security. Dedicated firewalls and routers in the extranet are the result of a highly secure and scalable network infrastructure for partner connectivity, yet if there are only a small number of partners to deal with, you can leverage the existing Internet Edge infrastructure. Some partners require direct connectivity or dedicated private links, and others expect secure connections through VPN links. The architecture of the server farm does not change whether you are designing Internet or intranet server farms. The design guidelines apply equally to all types of server farms, yet the specifics of the design are dictated by the application environment requirements.

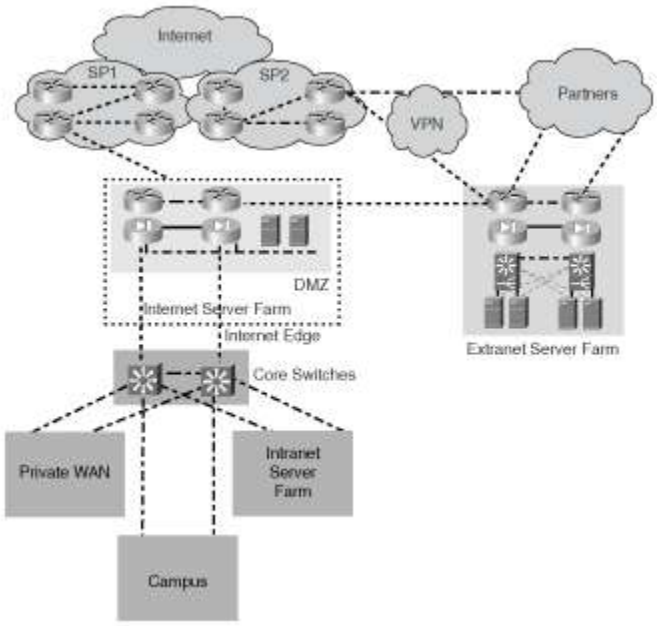

Figure 2-4: Extranet Server Farms

Corporate Data Center

Corporate or enterprise Data Centers support many different functions that enable various business models based on Internet services, intranet services, or both. As a result, support for Internet, intranet, and extranet server farms is not uncommon. This concept was depicted in Figure 2-1, where the Data Center facility supports every type of server farm and also is connected to the rest of the enterprise network—private WAN, campus, Internet Edge, and so on. The support of intranet server farms is still the primary target of corporate Data Centers.

Enterprise Data Centers are evolving, and this evolution is partly a result of new trends in application environments, such as the n-tier, web services, and grid computing, but it results mainly because of the criticality of the data held in Data Centers.

Server Farm Topologies and Network Infrastructure in Data Center:

Data Center Topologies

This section discusses Data Center topologies and, in particular, the server farm topology. Initially, the discussion focuses on the traffic flow through the network infrastructure (on a generic topology) from a logical viewpoint and then from a physical viewpoint.

Generic Layer 3/Layer 2 Designs

The generic Layer 3/Layer 2 designs are based on the most common ways of deploying server farms. Figure 2-5 depicts a generic server farm topology that supports a number of servers.

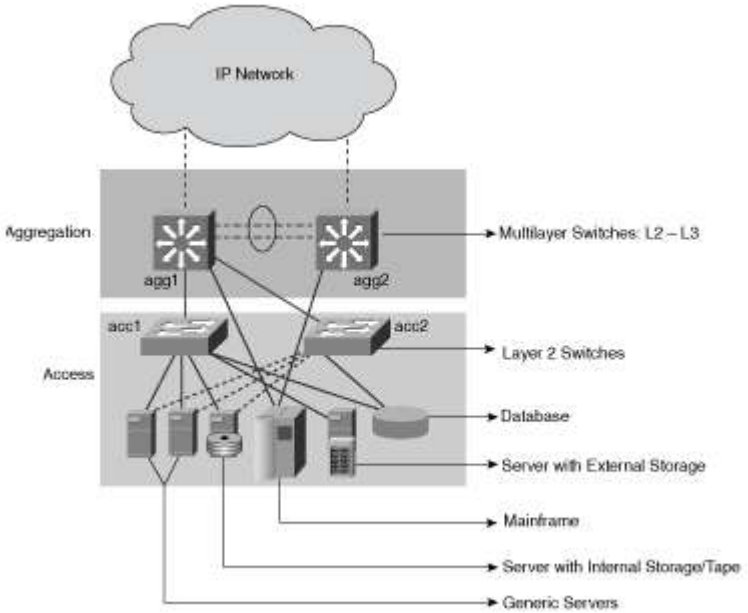

Figure 2-5 Generic Server Farm Design

The highlights of the topology are the aggregation-layer switches that perform key Layer 3 and Layer 2 functions, the access-layer switches that provide connectivity to the servers in the server farm, and the connectivity between the aggregation and access layer switches.

The access-layer switches provide direct connectivity to the server farm. The types of servers in the server farm include generic servers such as DNS, DHCP, FTP, and Telnet; mainframes using SNA over IP or IP; and database servers. Notice that some servers have both internal disks (storage) and tape units, and others have the storage externally connected (typically SCSI).

Multiple-Tier Designs

Most applications conform to either the client/server model or the n-tier model, which implies most networks, and server farms support these application environments. The tiers supported by the Data Center infrastructure are driven by the specific applications and could be any combination in the spectrum of applications from the client/server to the client/web server/application server/database server. When you identify the communication requirements between tiers, you can determine the needed specific network services. The communication requirements between tiers are typically higher scalability, performance, and security.

Figure 2-6 introduces a topology that helps illustrate the previous discussion.

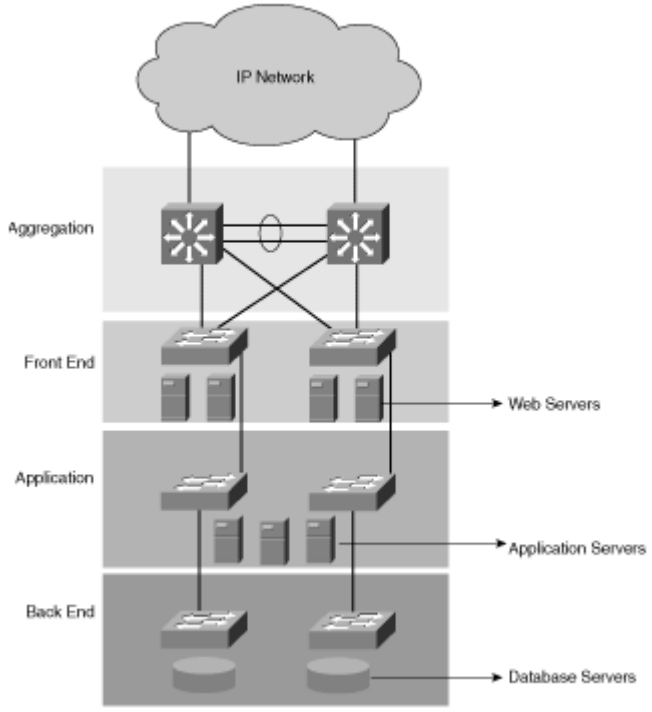

Figure 2-6 Multiple-Tier Application Environments

Notice that Figure 2-6 is a logical diagram that depicts layer-to-layer connectivity through the network infrastructure. This implies that the actual physical topology might be different. The separation between layers simply shows that the different server functions could be physically separated. The physical separation could be a design preference or the result of specific requirements that address communication between tiers.

For example, when dealing with web servers, the most common problem is scaling the web tier to serve many concurrent users. This translates into deploying more web servers that have similar characteristics and the same content so that user requests can be equally fulfilled by any of them. This, in turn, requires the use of a load balancer in front of the server farm that hides the number of servers and virtualizes their services. To the users, the specific service is still supported on a single server, yet the load balancer dynamically picks a server to fulfill the request.

Cable Management

General Construction

The construction and/or expansion of a Data Center must be done right the first time. You cannot afford delays or interruptions to return and correct a poor installation.

Access Raised Floor

An access floor is actually a floor raised above a floor. It's purpose is to create a chamber for wire management and the distribution of heating and cooling services.

In today's Computer Room environment, many pieces of electrical equipment are being used. Each of these have/require numerous power cords and cables. Your access floor creates an interstitial "holding" place for these cords and cables. In addition, this space can provide a method of distributing conditioned air to workstations above the floor through diffusers (or vents) placed throughout the access floor.

The construction of an access floor is comprised of 24" square and 1 7/16" thick panels. Air modules and diffusers built into a panel distribute HVAC (heating and cooling) services. These panels are easily interchangeable which, in turn, permit quick wire and cable management changes without disrupting ongoing operations. The floor panels can be rearranged at any time to suit your Data Center needs.

Figure 2-7 : Typical Raised Floor

Under floor Water Detection

Moisture below the floor can damage wiring or equipment and cause costly downtime. An under floor water detection system can give you an immediate warning. One with LCD display will show you the exact location of the leak reducing the chance of costly damage. The location of the leak is displayed on the control panel so you can use your time to resolve the leak rather than looking for it.

Structured Cabling in Data Centers

Over past several years, enterprise data centers have been installed using a wide variety of methods for connecting the contained electronics, resulting in a large tangle of cables that runs the risk of accidental damage and system downtime. To eliminate the clutter and provide a robust, scalable data center cabling infrastructure, new structured wiring solutions are available that provide for future growth and support rapid changes.

Data center design should follow industry standards for best practices. Industry guidance is on the way in the form of an emerging industry standard for data centers. This module lists requirements and provides recommendations for data center design and construction. As with ANSI/TIA/EIA-568-B.1-2001, *Commercial Building Telecommunications Cabling Standard*, which provides guidance on infrastructure design in local area networks, helps consultants and end-users design an infrastructure.

Figure 2-8 shows the main elements of the data center. The entrance room provides the interconnection point between the data center and the outside network. Service provider connections enter the data center through this room. In many data center designs, this area is located directly inside the computer room, or it may be in a separate room as shown in Figure 2-8. The computer room houses the bulk of the data center space. This space is where the switches, servers and Input/Output (I/O) are located. I/O equipment includes backup tape farms, storage, removable backup storage drives and Storage Area Networks (SANs). Also note in Figure 2-8, the Zone Distribution Area (ZDA). ZDAs pre-wire the data center and allow simple moves, adds and changes without disrupting the general computer room. Cabling changes therefore impact only the small area served by the zone.

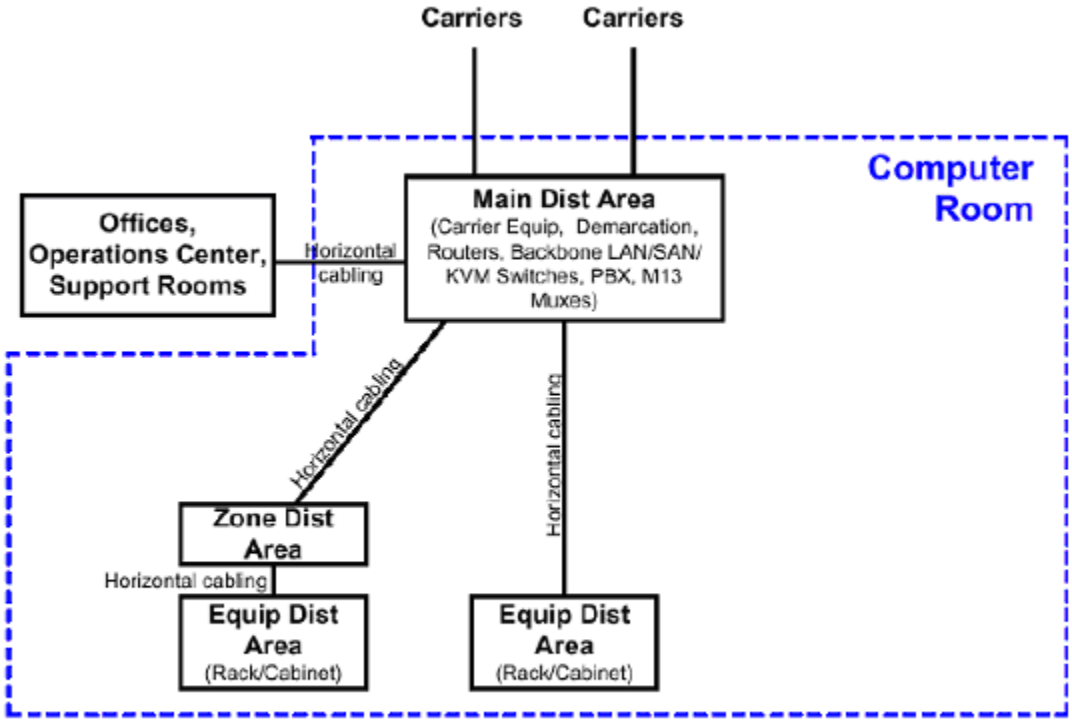

Figure 2-8: Example of Data Center Topology

Optical fiber cable is the media of choice for a number of reasons. Optical fiber cable provides the greatest bandwidth of all media types. Fiber is immune to EMI and RFI, doesn't require grounding, is much less expensive than copper cabling for the available bandwidth, and unlike copper, optical fiber can scale from 10 Mb/s to 10,000 Mb/s. Fiber cabling media is recognized by the industry cabling standards, among them TIA/EIA-568, Fiber Channel and IEEE 802.3. Multimode fibers with a 50 µm core size offer the best bandwidth/cost/performance solution available. While longer than most data center cabling runs, 10 Gb/s traffic can go 300 meters.

Begin your assessment by examining the components that make up the cabling infrastructure in the computer room. From Figure 2-9, the main areas are the Main Distribution Area (MDA), the Equipment Distribution Area (EDA) and the ZDA. The MDA contains core routers and switches (located near the MDA to minimize cable lengths) and the Fiber Distribution Frame (FDF), a line of equipment cabinets or racks containing optical fiber patch panels. The FDF serves as the central administration point for all functional areas in the data center. All of the optical cabling in the computer room feeds back into this area. In the MDA, free-standing equipment cabinets are common for holding the rack-mounted cross-connect patch panels or electronics.

The connector panels let end-users add capacity as needed in affordable increments, and connector type can be changed by simply removing the panel and snapping in a new one, eliminating the need to remove the patch panel housing. Connector panels have 1- or 2-fiber connector ports on the face of the panel. The panels come in 6-, 8-, 12-, 16- and 24-fiber increments and are fast to bring online since the installer simply snaps them into an unused spot in the housing and plugs the preterminated cables into the back of the panel. Cross-connect or equipment patch cords are then added to the front as needed. Connector panels are available in the standard data center.

Connectors – ST compatible, SC duplex, MT-RJ and LC duplex.

Patch panel housings used in the FDF contain provisions for attaching the cables entering the rear of the housing. The cable attachment device must be strong enough to withstand accidental pulling and twisting of the cable outside of the housing. The patch panel will also have patch cord management rings that maintain fiber minimum bend radii and facilitate orderly arrangement of the patch cords as they exit the housing.

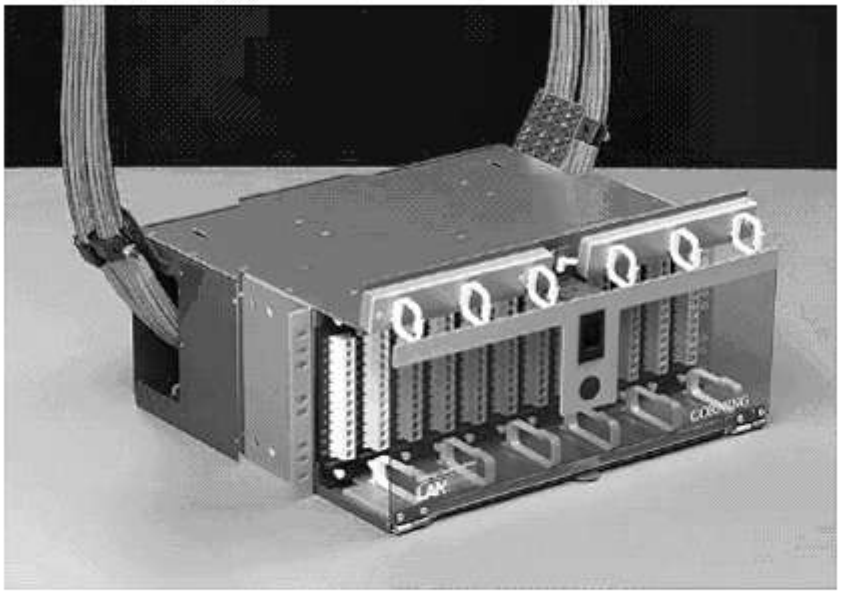

Figure 2-9: Fiber Distribution Frame

The next element of the data center is the ZDA. This area provides the interconnect point between the FDF and the EDA. The ZDA may be an equipment cabinet or rack, or it could be a smaller housing mounted on the building column, in the ceiling or under the access flooring. This area does not contain electronics. If the ZDA is serving a large number of ports it should be a cabinet or rack.

The final area is the EDA. Equipment cabinets or racks like the ones used in the FDF are used here. The difference is that the patch panels are 1U tall (1.75 inches) instead of 4U since the fiber count is smaller and space is at a premium. Connector modules are used in the 1U housing but are mounted horizontally instead of vertically due to height limitations. A removable top cover and hinged front and rear doors provide access to the connectors inside the housing. Connecting these areas together is the horizontal cabling. This cabling is located under the access flooring in well-defined pathways using a basket tray or cable tray to keep cables off the slab floor.

Module 3

Electrical Power Requirement

Data Center Design in the New Millennium

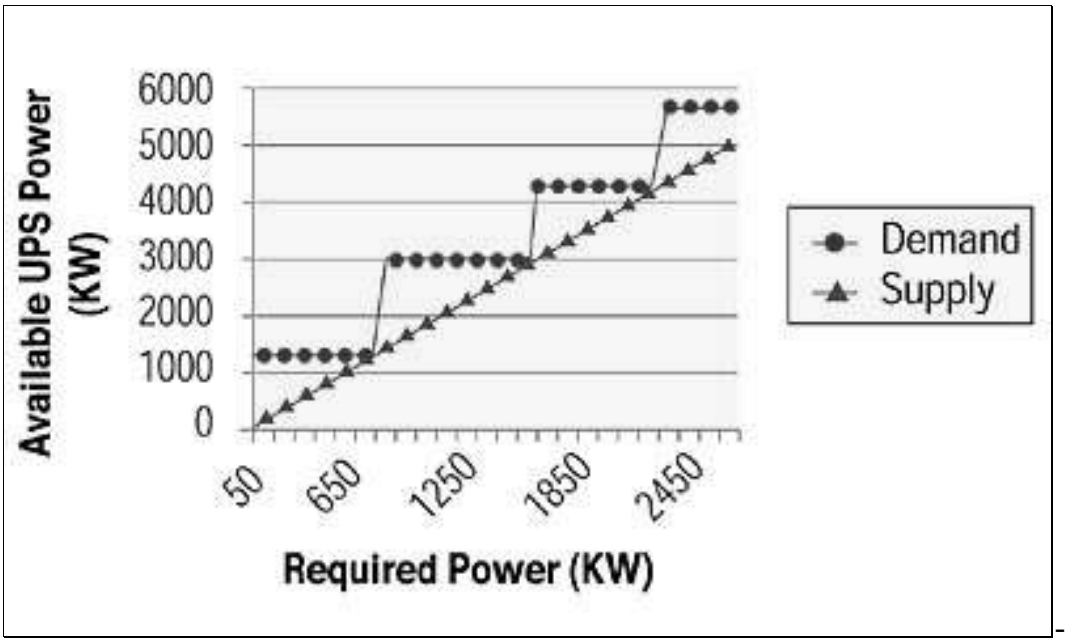

Figure 3-1: Power Requirement for Data Center

Today's rapidly changing marketplace makes designing data centers and facilities that meet the needs of today and tomorrow increasingly difficult. Time and money have always been an important part of the design process; however, increased dependence on corporate data centers makes system availability one of the most important considerations. For many companies, the entire corporate business process comes to a halt when a data center is down; even a brief outage can cause irreparable damage.

Sizing the electrical service for a data center or data room requires an understanding of the amount of electricity required by the cooling system, the UPS system, and the critical IT loads. The power requirements of these elements may vary substantially from each other, but can be accurately estimated using simple rules once the power requirements of the planned IT load are determined. In addition to estimating the size of the electrical service, these elements can be used to estimate the power output capacity of a standby generator system, if one is required for the data center loads.

Most data centers are part of a larger building. The steps in determining the electrical capacity described below will assist in estimating the capacity required for that portion of the building dedicated to the data center or data room. The difference between the steady state power and the peak power is important when calculating power capacity requirements.

Critical loads

A proper planning exercise in developing a data center, from a single rack sized environment to a full scale data center begins with determining the size of the critical load that must be served and protected. The critical load is all of the IT hardware components that make up the IT business architecture: servers, routers, computers, storage devices, telecommunications equipment, etc., as well as the security systems, fire and monitoring systems that protect them. This process begins with a list of all such devices, with their nameplate power rating, their voltage requirements, and whether they are single phase or three phase devices. The nameplate information must then be adjusted to reflect the true anticipated load. The nameplate power requirements are the worst-case power consumption numbers required by Underwriter's Laboratory and in almost all cases, are well above the expected operating power level. Studies conducted indicate that the nameplate rating of most IT devices is well in excess of the actual running load by a factor of at least 33%. The U.S. National Electrical Code (NEC) and similar worldwide regulatory bodies also recognize this fact and allow electrical system planners to add up nameplate data for anticipated loads and multiply by a diversity factor, anticipating that not all devices are running at full load 100% of the time.

A. Add up the nameplate power of the anticipated loads. If the wattage is not listed on the device, it can be determined by multiplying the current (amps) by the voltage of the device to get the VA, which approximates the amount of watts the device will consume.
B. Multiply the anticipated VA number by 0.67 to estimate the actual power, in watts, that the critical load will represent.
C. Divide the number by 1000 to establish the Kilowatt (kW) load level of the anticipated critical load.

Future loads

Data Center loads are not static. Once built or established, the IT equipment will be under an almost constant state of change during the lifetime of the data center. Information Technology at a minimum, have a 3 year cycle where new, more powerful or efficient devices will be installed with, or replace the devices. A realistic assessment of the scope and timing of future changes and upgrades should be developed by the IT organization to allow proper planning for the initial determination of power requirements. Future loads, or provision has to be made for installing additional capacity without incurring excessive downtime that would adversely affect the availability expected by the IT customer. Once an estimate is made for the amount of future loading, it is added to the base loading information developed above to establish the electrical critical load number in kW.

UPS loads
Assuming that the availability determination in the needs assessment, explained above, requires the inclusion of UPS power (in almost all cases this is true), the total electrical load power must include a factor for the inefficiency of the UPS system as well as the additional power required for battery charging.

Lighting loads
Lighting loads account for all the lighting in the data center portion of the building and are a function of the data center floor area. A good rule of thumb for this type of load is 3 watts per square foot.

Cooling loads
Note that cooling loads have startup peak loads that exceed the steady state values which are accounted for in this calculation.

Sizing the electrical power system

Two important numbers have been determined that will assist in estimating the size of the electrical system that will power the data center environment: the Total Critical Load and the Total Cooling Load. In general, the electrical supply must be large enough to support the sum of these two numbers, plus the related data center lighting loads. The steady-state power consumption of the loads within a data center establishes the power consumption for purposes of determining electrical costs. However, the Electrical Service and the Generator power sources that provide power to the data center cannot be sized to the steady state values. These sources must be sized to the peak power consumption of the loads, plus any derating or over sizing margins required by code or standard engineering practice. In practice, this causes the electrical service and generator sizing to be substantially larger than might be expected, as will be illustrated in the next section.

Final Electrical Capacity Computation
Once the total electrical capacity is estimated in Kilowatts from the process described above, two critical determinations can be made: the first is an estimate of the electrical service needed to supply the data center, and the second is the size of any standby power generator capacity that may be needed to achieve the desired availability.

Sizing of the Electrical Service

The electrical service can be calculated as follows:
1. Take the total electrical capacity required in Kilowatts and multiply by 125% to meet the requirements of the National Electrical Code and similar regulatory bodies.
2. Determine the three phase AC voltage of the service entrance to be supplied by the utility company.
3. Use the following formula to determine the electrical service size to supply the data center, in Amps:
Amps = (kW x1000) / (Volts x 1.73)

This provides an estimate of the electrical service capacity required to support the critical load, cooling, and the building functions for a data center. It must be noted that this is only an estimate, and that the final determination of the service size is highly dependent on accurate site specific information.

Cooling Requirement:

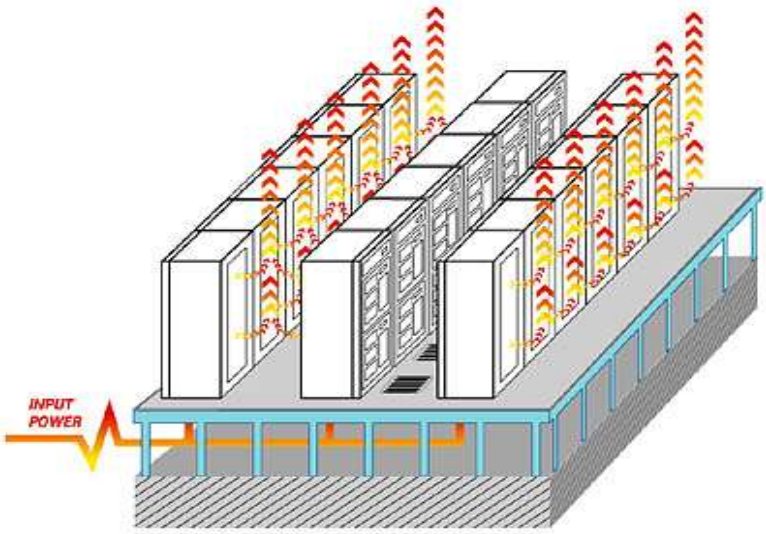

Figure 3-2: Power distribution under the floor

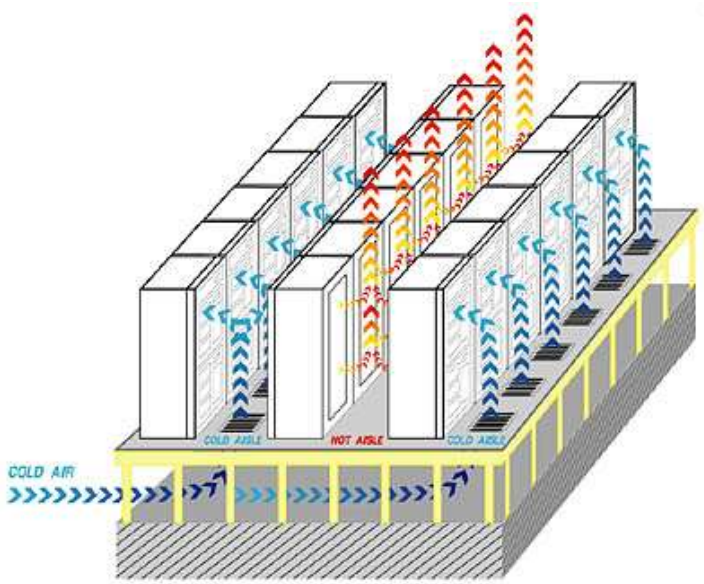

Figure 3-3: Air distribution under the floor

The designer of a facility or data center first encounters some new challenges affecting availability during design and build-out. Over that lifetime, the equipment in the room will be replaced four to five times with new generations of equipment. The rapid change of the equipment makes even the most basic future estimates of size and capacity almost impossible. Moore's law has produced microprocessor transistor counts that double every 18 months. With each generation, the additional transistors require almost proportionately more power. Accordingly, microprocessor heat output has gone up significantly. Intel's new Pentium 4 chip produces about 100 watts (W) of heat compared to the 80486 chip, which produced less than 10 W. Increasing chip density has magnified heat production at the same rate. These changes have led to data center design power density requirements of greater than 150-200 W per square foot. Accordingly, system infrastructures have expanded tremendously to support both the electrical and cooling requirements of the data center loads.

Failure to predict future electrical needs leads to one of the most significant data center problems: the inequality of supply and demand for highly available power. Not only does this inequality reduce the efficiency, utilization, and support capabilities of the data center, but it also impedes optimal capital usage.
For example, when a large data center is built-out, it often takes two to four years before the site is running at or near desired capacity. Therefore, for the first few years of operation there is little demand for highly available power.

The Consequences

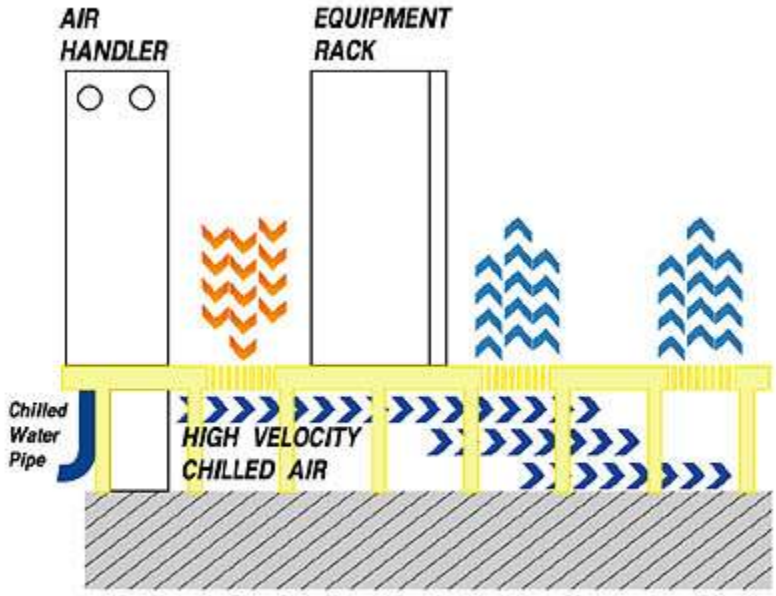

Figure 3-4: Alternating hot and cold aisles increases efficiency.

In some cases, the user will have spent millions of dollars building the site to full capacity, including purchasing a multi-megawatt redundant power system to support the center.

On a rack basis, power density has increased from 1.5-2 kW per rack to 3-4 kW in about a year's time. Newer blade-based servers could raise power density even higher. New data centers sometimes require a major overhaul in just four years.

While new air handlers can often be placed on the present raised floor, the height of the raised floor may not be sufficient to support the additional airflow. In particular, the rising number of power and data cables, combined with larger chilled water pipes, can inhibit proper air flow under the floor and prevent adequate static pressure to cool the high-density equipment.

Adding additional perforated tiles in front of the appropriate equipment leads to mixed results, often increasing cooling at one point, but reducing static pressure in other areas and creating hot spots.

The Different Types of UPS Systems
There are two most common type UPS systems used:

- Standby UPS Systems
- Line Interactive UPS Systems

- **Standby UPS System:**

The Standby UPS system is the most common type used for personal computers and stand alone networking hardware like Switches, Routers and also for stand alone servers used for testing.

In this type of UPS, the transfer switch is set to choose the filtered AC input as the primary power source and it switches to the battery as a backup source when the primary source fails. The inverter starts only when the power fails, hence it is called “standby”. High efficiency, low cost and small size are the main benefits of this design.

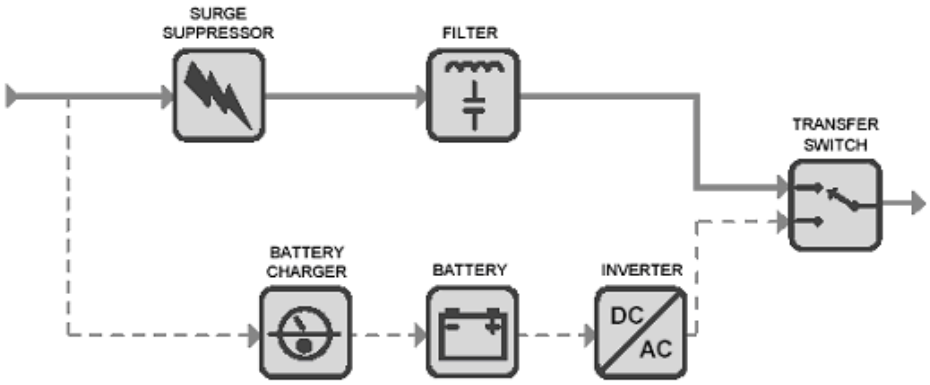

Figure 3-5: Standby UPS System

- **Line Interactive UPS System:**

The Line Interactive UPS system is the most common type used for businesses and Data Center use. In this design, the inverter is always connected to the output of the UPS., which provides battery charging.

When the input power fails, the transfer switch opens and power flows from the battery to the UPS output. With the inverter always on and connected to output, it provides additional filtering and reduces switching transient.

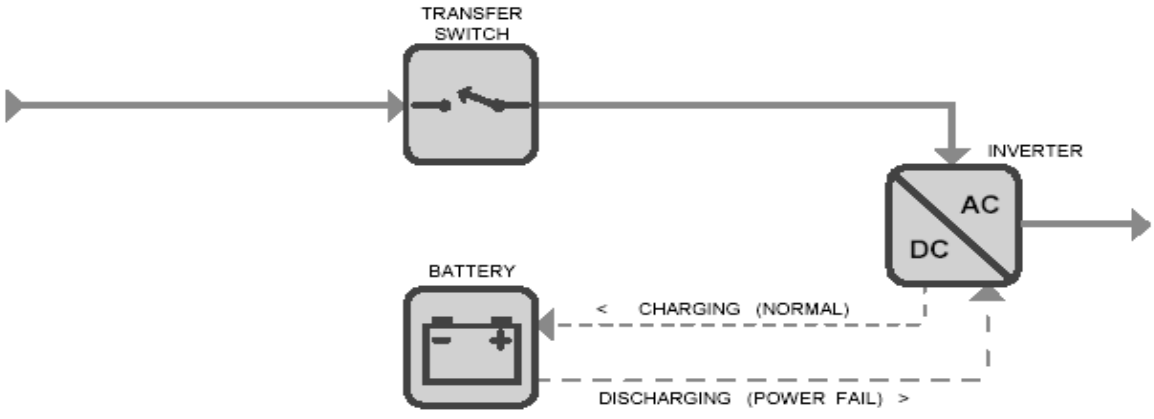

Figure 3-6: Line Interactive UPS System

While determining the size of the UPS systems, the following considerations to be made:

- Which Servers/Racks are critical and must be on UPS power
- How long the battery power needed
- Future expansion plans

Generator Systems:

In current business environment, Data Center availability is very critical. Few hours of Data center downtime can affect the profitability of business very significantly.

Engineering point of view, Generator system is designed using Automatic Transfer Switch(ATS) which means, when normal power fails signal is sent to Generator system and Data Center is fed from Generator power via ATS. Designer should specify a Remote Annunciators panel in the Data Center with LED display to display when the Generator turns on. In the event of power failure, responsible personnel must be notified too.

Generator systems must be tested every one to three months to ensure its functionality in the event of power failure.

Standby power generation is a key component of a high availability power system for data centers and network rooms. Information technology systems may operate for minutes or even a few hours on battery, but local power generation capability is key to achieving high availability. In locations with poor utility power, local power generation may be needed to achieve even a minimal requirement of 99.9% availability.

Generator systems with diesel or natural gas engines are, in most cases, the solution for standby power generation. A generator system includes not only the standby generator, but also the automatic transfer switch (ATS), the output distribution, and the communication or management system as shown in Figure 3-7.

The ATS is fed by two sources, the utility and the generator, with the utility the preferred source. When the preferred source is unacceptable, the ATS automatically switches to the generator.

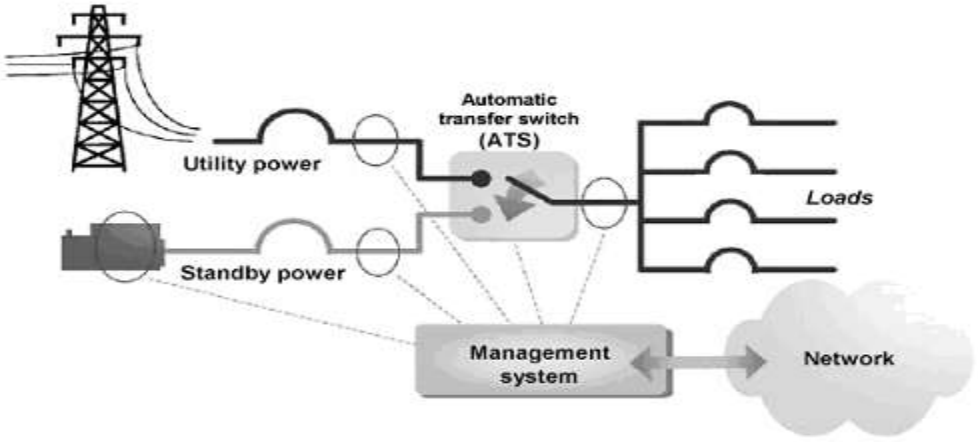

Figure 3-7: Standby Generator System

Standby generator systems are typically used in conjunction with UPS systems. There are several issues that need to be considered when choosing, installing and operating a generator system that operates seamlessly with a UPS.

In the past, network infrastructure such as UPS and generator systems were solely the responsibility of facilities managers. However, two trends have led to a convergence of facilities and IT.

1. Data centers have become more critical to the profitability of businesses (i.e. downtime is very expensive), which has led IT managers to take more responsibility for the UPS and generator systems. IT managers are bringing these systems closer to the equipment racks in order to decrease the single points of failure between them and the critical loads.

2. Data center power densities are increasing, which has placed a greater importance on cooling critical loads during power outages. When a power outage occurs, the UPS system maintains the critical load; however the cooling system will not resume operation until after utility power returns. Data centers with high density racks cannot sustain a long cooling outage and will shut down before cooling has resumed.

Since IT managers are ultimately responsible for the critical data processing that takes place in their data centers, they are becoming more involved in the specification and operation of generator systems. The challenges presented in this paper are largely based on traditional generator systems tend to offer too many options and design choices. The many available alternatives often leads to delays in installation, unnecessary engineering costs, and less reliable systems.

Generator System Challenges in Mission Critical Installations

A comprehensive analysis of data center and facility managers with mission critical installations was conducted to identify key challenges associated with choosing, installing and operating standby generator systems. These core challenges were then further grouped into five key theme areas:
• Manageability
• Availability / Reliability
• Maintenance / Serviceability
• Lifecycle cost
• Adaptability

Fire Protection

Choosing a Fire Protection Solution For the purposes of designing a fire protection solution for a data center, three conditions should be met; identify the presence of a fire, communicate the existence of that fire to the occupants and proper authorities, and finally contain the fire and extinguish it if possible. Being familiar with all technologies associated with fire detection, alarming, and suppression will ensure a sound fire protection solution.

Fire Detection System Types
Three main types of detectors are available; smoke detectors, heat detectors and flame detectors. For the purposes of protecting a data center, smoke detectors and heat detectors are far more effective. Spot type smoke detection Spot type smoke detectors can cover an area of about 900 square feet (84 square meters). These types of detectors aren't intelligent enough to be desensitized or report their locations therefore are ineffective in a data center. There are two types of spot type detectors; photoelectric and ionization. Photoelectric detectors work by using a light source and light sensor perpendicular to it. When nothing is in the chamber the light sensor doesn't react. However when smoke enters the chamber, some of the light is diffused and reflected into the light sensor causing it to sound the alarm.

Ionization detectors use an ionization chamber and a small amount of radiation to detect smoke. Normally the air in the chamber is being ionized by the radiation causing a constant flow of current, which is monitored by the detector. When smoke enters the chamber it neutralizes the ionized air thereby causing the current to drop. This triggers the detector into an alarmed state.

Fire Suppression System Types
Once a fire is detected in a data center, it is critical to quickly extinguish the fire with no effect on the data center operation. To do this various methods can used, some better then others. Regardless of the method employed, it should provide a means to abort the suppression system in the event of a false alarm.

Foam
Foam formally called, Aqueous Film-Forming Foams (AFFF), is generally used in liquid fires because when applied it floats on the surface of the flammable liquid. This prevents the oxygen from reaching the flames thereby extinguishing the fire. Foam is electrically conductive therefore couldn't be used anywhere where electricity is present. Needless to say it should not be used in data centers.

Dry chemical
Dry chemical or dry powder systems can be used on a wide variety of fire and pose little threat to the environment. Different types of powders can be used depending on the type of fire. They are electrically nonconductive but require clean up. They are used in many industrialized applications but are not recommended for data centers due to the residue left after discharge.

Water sprinkler systems
Water sprinkler systems can be installed in three different configurations: wet-pipe, dry-pipe, and pre-action. Dry-pipe systems are charged with compressed air or nitrogen to prevent freezing. Pre-action systems prevent accidental water discharge by requiring a combination of sensors to activate before allowing water to fill the sprinkler pipes. Normally water sprinklers are not recommended for data centers; however, depending on local fire codes they may be required. In this case a pre-action system would be recommended.

Water Mist Systems
Water mist systems discharge very fine droplets of water onto a fire. Water mist systems are gaining popularity due to its effectiveness, however, it remains to be seen whether or not water mist systems will one day protect data centers.

Fire Extinguishers
Sometimes the oldest method of fire suppression is the best. Fire extinguishers these days are essentially the same as that have always been in that they are easy to use and can be operated by just about anyone. What makes fire extinguishers so valuable to data centers is the ability to extinguish a fire before the main suppression system discharges..

Security:

In new technology era, subject of security is very wide, and here we will discuss it very briefly just to familiarize the designer.

Physical security — controlling personnel access to facilities — is critical to achieving data center availability goals. As new technologies such as biometric identification and remote management of security data become more widely available, traditional card-and-guard security is being supplemented by security systems that can provide positive identification and tracking of human activity in and around the data center.

Defining the Problem
Secure Areas:
The first step in mapping out a security plan is just that — drawing a map of the physical facility and identifying the areas and entry points that need different rules of access, or levels of security.
These areas need to be secured:
Building perimeter
Computer area
Computer rooms
Equipment racks
Visitor areas
Offices
Utility rooms
Three basic types of security methods are used besides cameras and security alarm systems:

- Magnetic strip cards
- Bio Metrics
- Key pad type locks.

Top Ten Data Center Design Guidelines:

1. Plan ahead. You never want to hear "Oops!" in your data center.

2.Keep it simple. Simple designs are easier to support, administer and use. Set things up so that when a problem occurs, you can fix it quickly.

3. Be flexible. Technology changes. Upgrades happen

4. Think modular. Look for modularity as you design. This will help keep things simple and flexible.

5. Use Rack units, not square foot. This will help for better capacity design.

6. Worry about weight. Servers and storage equipment for data centers are getting heavier every day.

7. Use Aluminum tiles in the raised floor system. Cast aluminum tiles are strong and will handle increasing weight load requirement.

8. Label everything. Particularly cabling!. Lot of time will be saved later while fixing the problems and you will have to trace bad cables.

9. Keep things covered or bundled. This way it can not be messed with.

10. Hope for the best, plan for the worst. That way, you are never surprised.