

FACILITIES AND IT



LAD ENTERPRIZES, INC.
www.ladenterprizes.com
610-429-3122

June 2009

Written By: Dave Burford

Facilities and IT

Miscommunication between IT and Facilities Groups can be disastrous for a data center's welfare.

By Stephen J. Bigelow

A building's Infrastructure is frequently overlooked by management when it comes to its Information Technology initiatives and needs. However, successful implementation of Information Technology solutions is dependent on the building environment and available resources.

What do buildings provide Information Technology?

- Electric Power
- Climate Control
- Communication Infrastructure
- Space, Environment and Physical Security

Modern building codes and utility companies combine to make meeting these needs almost ubiquitous in our day-to-day lives. However, technology places special demands on facility infrastructure; demands that are frequently overlooked and unmet.

ELECTRIC POWER

Commercial electric supply is so reliable and omnipresent that we hardly think about it. It seems like it is "always on". Yet it is the essential raw material that is consumed by Information Technology and the key operating resource representing the largest operating cost for IT/Communications equipment. Any interruption of current shuts down electrical equipment. Without it we don't communicate and we don't use computers.

Electrical power problems are a likely disaster scenario threat for IT.

To use IT equipment without experiencing induced outages and data loss you must have reliable high quality electrical power (at the building) with enough Amps at the correct voltage available at the production location (the circuit within the building) to run your IT equipment.

In a perfect world, commercial AC power is delivered at a constant voltage and appears as a smooth, undistorted symmetrical sine wave varying at a specified number of cycles every second. The United States

is standardized at 120 Volts (V) and 60 Hz as published by The Institute of Electrical and Electronic Engineers Inc (IEEE). Unfortunately we don't live in a perfect world.

Consider even if workstations are shut down nightly, most servers, switches and modem equipment run 24/7/365 – that's 31,536,000 seconds per year. Just one, one second power outage (well within the 6 Sigma standard strived for by most commercial power companies) shuts down this equipment ungracefully. Sometimes an ungraceful shutdown can be catastrophic, rendering an entire database – say your financial or e-mail data - corrupt beyond repair.

Power outages happen more often than expected. You may not be aware of power being shut off during off-business hours. We are often told by clients that outages don't occur only to find that over time power is cut off occasionally at night or on weekends and that these unplanned/unannounced outages cannot be controlled.

Power outages aren't the only potential problem. The quality of the AC power can be poor. We're all familiar with surges (too much voltage) and brown outs (not enough). APC identifies 7 problem categories arising from 13 different power disturbances. These can also result in data loss or equipment damage.

Consider the circuit. The circuit that supplies power also has to be able to support the equipment. For fire safety, building codes limit the amount of current (Amps) that a circuit can carry. Don't forget that most circuits service multiple outlets as well as overhead lights and many buildings have more than one room on a circuit. Per construction code, electrical circuits have 15 or 20 Amp breakers and fire codes further limit the load as an additional safety factor. These limits become an issue when the IT solution calls for multiple workstations or multiple servers. To illustrate: a Dell Optiplex 360 workstation is rated at 255Watts (W) or 2.125 Amps (A) at 120Vs. Five or six of these workstations could be safely run on a single circuit providing no other electric devices were in use. A Dell server (PE2900) is rated at 930W or about 7.75A at 120V. Only one of these servers should be installed on a 15 Amp circuit. These examples don't include other required IT equipment such as monitors, printers or switches nor common workplace equipment such as calculators, copy machines or pencil sharpeners.

CLIMATE CONTROL

Heat is the byproduct of consumed electrical power and is produced by all electrical devices. This heat must be removed to prevent equipment temperature from rising to an unacceptable level and ultimately damaging the equipment.

After power outages, heat is the source of the second most likely disaster scenario threat for IT – thermal events.

Electric power consumed by IT equipment is essentially all converted to heat. This fact allows the thermal output of IT equipment in Watts to simply equal its power consumption in Watts. Thus, the total heat output of a system is the sum of the heat outputs of the components.

IT equipment produces an unusual, concentrated heat load, and at the same time, is sensitive to changes in temperature or humidity. Typically, equipment is designed to operate in conditions of 72-75°F and 35-50% relative humidity. Additionally moisture should not condense on equipment. Even if heat does not cause equipment to shut down, temperature variations can alter the electrical and physical characteristics of components, causing reduced equipment life, faulty operation or premature failure.

IT equipment is typically air-cooled. Fans force hot air out of the equipment into the room while drawing cool room air inside the equipment. Unless the excess heat energy is removed, room temperature rises until IT equipment fails. This situation can rapidly become critical when IT equipment is placed in an inadequately ventilated high density installation, such as in a server room or wiring closet. To illustrate, the Load Density of office space ranges from 5-15W/ft² while a technology room ranges from 50-200W/ft².

Unfortunately, commercial A/C systems are not designed to address the load density, temperature or humidity set point tolerances, or year round/all weather operation required for thermal protection of technology. For example, many buildings do not offer A/C during winter months or have thermostats located away from the “hot spot” associated with the IT equipment.

Specialized A/C equipment – called Precision Air Conditioners or Computer Room Air Conditioners (CRAC) – may be required. These cooling systems differ from residential or commercial A/C systems in that they provide more precise, stable environments by closely regulating air temperature and moisture (humidity). The system controls maintain room conditions for the full range of outside ambient conditions, summer or winter and are designed and built to run non-stop 8,760 hours a year with components selected and redundancy incorporated to ensure minimal downtime. They are frequently rated in Kilowatt Hours (kWh) making it easier to select the correct unit for the amount of heat to be removed. A useful rule of thumb for rooms under 4,000 ft² is to select a unit with a system rating 1.3 times the anticipated total load plus any capacity added for redundancy. These specialized units need to move heat to another location, preferably outside of the building.

COMMUNICATION INFRASTRUCTURE

Communication Infrastructure is the underlying base of an organization's data, voice and video communication systems. A reliable quality communication infrastructure is one of the most important requirements of business, only surpassed in importance by reliable high quality electrical power. A robust communication infrastructure provides increased productivity for any given organization.

In general there are two media over which communications travel: cable, and radio (wireless). Both media are heavily regulated and the characteristics of the building itself impact the reliability and quality of the communications experience.

The facility building construction material greatly impacts the communication solutions installation and availability. Concrete, cinder block, or stone wall/floors limit/block wireless signal penetration and can make difficult or impossible post construction cable installation. Chain link, grating, steel or other metal wall/floor materials also block or reflect wireless signals and also can present challenges to cabled solutions. If the facility is very large or is a campus of separate buildings, the physical distance that signals must travel can either limit or dictate the communication solution.

In North America, specifications for power and cooling capability are still often provided in the legacy BTU and Tons terms.

Start Unit	Conversion Factor	End Unit
BTU/hr	0.293	Watts
Watts	3.41	BTU/hr
Watts	0.000283	Tons
Tons	3,530	Watts
Tons	12,000	BTU/hr

Because of the severe performance and potential reliability/security issues associated with wireless systems, from an IT networking perspective, cabled solutions are always preferred over wireless solutions.

Cable has two mediums: copper (electrical signals), and fiber (optical signals). Cable, when properly installed, is extremely reliable and has a long service life. Some of the transport technologies include Cat-5e, Cat6, single and multi-mode fiber and coax. Each of these technologies exhibits their own characteristics, capabilities and prices. To support technologies such as Fast Ethernet (100BaseT Ethernet), Gigabit Ethernet, and fiber, cabling systems require care and planning prior to and during the install. Placement of components can be critical to success.

Figure 1 on the next page illustrates the installation. The drop, in-wall cable and patch panel components of the installation become part of the building. By connecting the patch panel jacks to a switch, the full speed potential of the cables can be used by large numbers of network devices without any data loss or interruptions.

Patch panels, connectors, and jacks should be installed and cable pulled to EIA/TIA standards or communication quality and reliability can suffer. Copies of ANSI/EIA/TIA commercial building cabling for telecom products and services standards (ANSI/TIA/EIA-568-B.1-2001, -B.2-2001, and -B.3-2001) can be

purchased from the TIA website (<http://www.tiaonline.org/standards/catalog/index.cfm>). Local Building standards and codes may also play a role – requiring, for example, plenum cabling for fire safety – and may prohibit installation except by permit or licensed installers. ***Because of the complexity, we recommend using an Electrician or Cable installer experienced in the medium (fiber or copper) and knowledgeable of local building codes.***

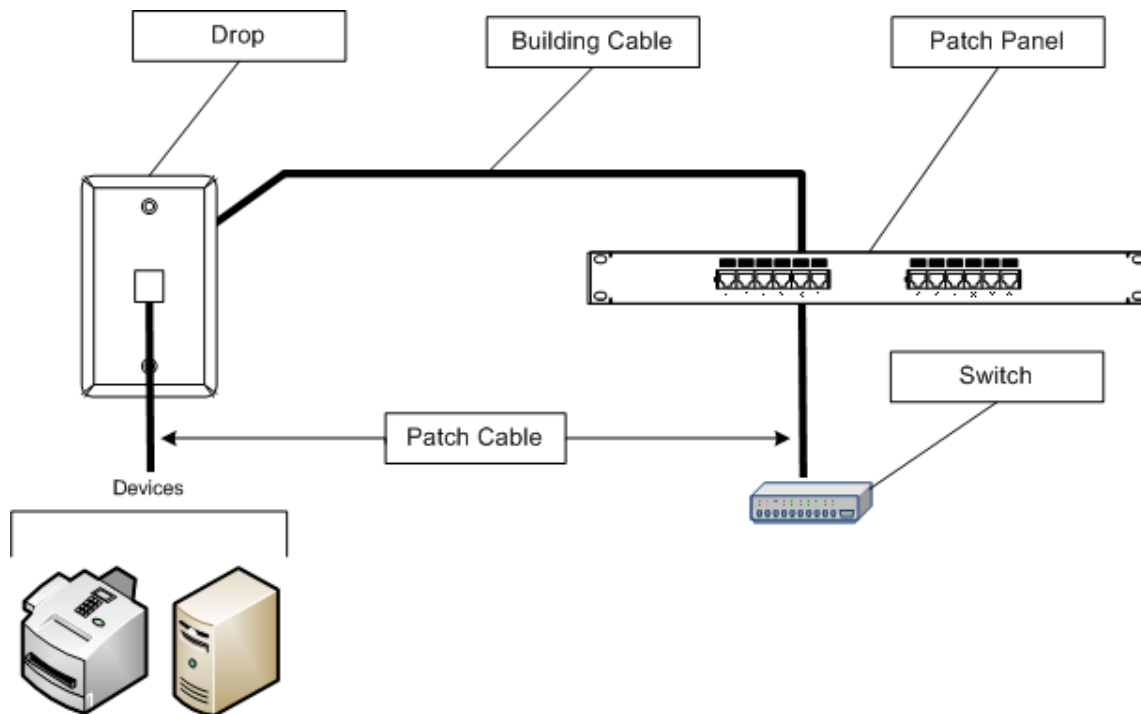


Figure 1

Wireless communications technology is simply two way radio and has all of the advantages and disadvantages of radio. In 1985 the US Federal Communications Commission freed three bands of the wireless spectrum, albeit broadcasting at low power, to be used without a license: 900MHz, 2.4GHz and 5.8GHz. Current wireless networks use radio technologies governed by the Institute of Electrical and Electronics Engineers (IEEE) standard IEEE 802.11. Typically a wireless solution includes one or more wireless access points (WAPs) and one or more clients broadcasting on the 2.4GHz band (WiFi) or more recently the 5.8 GHz Band. The WAP broadcasts it's SSID (service set identifier, or "network name" called a beacon), usually every 100 ms. This beacon is transmitted at 1 Megabits per second (Mb/s). The client detects the beacon and connects and negotiates the speed with the WAP. Since 1 Mb/s is the lowest speed of Wi-Fi, theoretically a client device that receives the beacon can communicate at the slowest speed.

In the real world, about half of the wireless bandwidth is consumed by overhead traffic required to establish and maintain the communications link and network speed falls rapidly as a function of distance from the WAP. Signal interference by nearby devices and data collisions arising from 2 devices

communicating simultaneously also reduce speed. It is very easy to have intermittent connection problems using wireless technology.

SPACE, ENVIRONMENT, AND PHYSICAL SECURITY

It might seem obvious, but you need enough room to house and appropriately secure IT equipment. Worker office space requires room for the computer, monitor, keyboard/mouse and perhaps a local printer. Sometimes ancillary equipment such as scanners, speakers or audio/video equipment may also need to be considered. Network printers and Multi-Function Printers require placement in more or less public space to be accessible to workers.

The real challenge for most organizations is finding appropriate space for servers, switches, network appliance devices, router/firewalls and Internet connection equipment (e.g. modems). Additional equipment such as racks, backup storage devices (server room placement is not recommended), UPS and batteries, and Computer Room Air Conditioning (CRAC) units may also be present. Storage for spare equipment may also be needed.

For the SMB, this room is the equivalent of the Data Center for a large organization. Many authorities name this space a Server Room, Computer room, IT room, or Wiring Closet.

Unfortunately, frequently this question is not asked until after equipment is selected, purchased and on premises. Just as frequently, expanding IT needs result in outgrowing the facility capability. The rest of this discussion focuses on what we will call the Server room.

Server Room Characteristics

Space: The floor area required for the server room is determined by the specific servers and other equipment to be installed, the location of columns, floor loading capacity, and provisions for future expansion. Ideally a Server room should accommodate all of your equipment with plenty of room for growth. Allow enough space for cabling and access to the side and back of equipment. Room height might need to be sufficient to accommodate a raised floor as well as the air-conditioning and ventilation ducts needed for the CRAC unit. Packing equipment too close together not only makes it difficult to work in the Server room, it also restricts air flow exasperating heat control efforts. The space should also allow rearrangement of equipment as needed, including adjustments in air conditioning and electrical power. The room should also be able to accommodate replacement equipment.

Noise: Servers are almost certainly too loud to place near or in an office/work environment. Server noise is rated between 50-90 db for comparison: speech is 40-70 db; office noise is 50 db; a train at 200 feet is 95 db and a lawn mower at 3 feet is 107 db.

Lighting: Sufficient proper lighting is required to normally operate the server and when service is required. This facilitates efficient operation and maintenance activities. Light sources in the Server room should have a general lighting level of 300 to 500 lumens/m² or 30 to 50 foot-candles.

Air quality: Servers and other Server room equipment are sensitive to air quality. Ensuring building air cleanliness may involve installing air filters. If you are installing your system in a typical business office or clean industrial location, you probably do not have to worry about the quality of the surrounding air. However, if your site is unusually dirty or has a chemical odor, you should be concerned. Dirt and corrosive gases can cause corrosion and possible equipment damage. This is particularly true over time. High concentrations of gases such as sulfur dioxide, nitrogen dioxide, ozone, and acidic gaseous chlorine associated with industrial processes are known to cause corrosion and failure of electronic components. In addition to gases, some industrial processes produce particulate contamination. These particles can settle (in the form of dust) in surrounding areas even though the process producing the particles might be some distance away. If oil or other petroleum product particle contaminants are also in the air, dust collection is accelerated. A high efficiency filter should be installed to filter all air supplied to the Server room.

Mechanical vibration: Some sites, such as those in or near large industrial factories, can experience vibration beyond the IT equipment rating. If you believe this is a risk, measure vibration amplitudes and spectra. A dampening technology or another location may be needed.

Communications Availability: The technology solution will require a variety of communication equipment to support the computer installation. Telephone lines, fax lines, and Internet access are some of the types of communications that may be needed. The solution should allow for expansion of network capabilities to ensure the right levels of performance (bandwidth, latency and uptime) at reasonable costs. It is wise to put a telephone in the Server Room to facilitate third party technical support.

Electrical supply: Sufficient multiple electrical outlets with appropriate circuit voltage and amperage is required and, when done well, facilitates future enhancements. Reliable high quality electrical power is required for the proper functioning of IT equipment. Consider the need for circuit protection, UPS, and backup generators.

Thermal/Humidity Control: Conduct a total heat load assessment to determine the overall environment balance point. The purpose of the assessment is to determine if there is enough room sensible cooling, including redundancy, to handle the heat load of the equipment to be installed. If not, create temperature and humidity design criteria to ensure that the room environment provides optimal conditions for equipment operation. A temperature control system should consist of

temperature and humidity controls providing a continuous record of the environmental conditions. These controls should be placed in a representative location within the server room. The air conditioning system must provide year-round temperature and humidity control to remove the heat created during equipment operation. Careful attention should be given to the method of air distribution to eliminate areas of excessive air motion and hot spots. Refer to the latest ASHRAE publication, "Thermal Guidelines for Data Processing Environments", dated January, 2004. This document can be purchased online at ashrae.org. A dedicated section outlines a detailed procedure for assessing the overall cooling health of the data center and optimizing for maximum cooling.

Accessibility, Location, Security: Select a room where it will be possible to place large, bulky, heavy equipment. The issue here is to think about how new equipment will be moved to the room for installation and if the room floor will structurally support the weight. Realize that a server might weigh more than 100 lbs and that a modest UPS with batteries may weigh more than 140 lbs.

Security experts suggest that physical security of technical equipment is a requirement to ensure a secure network. Try to select a room that has a door that can be locked. Avoid locations of the building with high walk-through traffic, for physical security reasons basement and ground floor levels are not recommended - avoid the risk of flooding in the basement and roof leaks on the top floors. Avoid locations where plumbing runs directly across the ceiling of the server room, or locations where a bathroom is overhead on the next upper floor – avoid the risk of leaks. Server rooms that border outside walls can make temperature and humidity control difficult, especially if they have windows. Look for locations that allow for expansion.

CONCLUSIONS

Even a small server installation can benefit from a dedicated Server room. Small servers can impose an intolerable noise and thermal burden in an ordinary office environment, and serious security concerns can arise from a server that offers easy physical access to individuals. A dedicated room can be equipped with specialized air conditioning to handle the substantial thermal burden imposed by the server and equipment configuration. A dedicated room also makes access control straightforward.

Real-world decisions require making trade-offs. We believe it is unusual for any server installation—particularly if it's the first for an organization—to proceed without challenges. Once the first physical server is installed, many organizations suddenly (or not so suddenly) realize that they need new services and capabilities. That recognition leads to unplanned demands for increased server or network capability in data handling, computing power and/or data storage. We suggest monitoring conditions and revisiting infrastructure decisions on a fairly regular basis. The environment (especially business requirements) may undergo changes that call into question earlier decisions, resulting in a need to analyze the potential

benefits, risks and costs of change. A review process allows you to analyze your IT solutions on a daily basis and evaluate proposed improvements and fixes. This is not to suggest using complex bureaucratic process with a specialized audit team. Instead, a simple process tuned to the size and capabilities of your business and IT solutions is best, letting you measure and review certain operational characteristics.

If a server room is not feasible due to budget or space constraints, consider custom cabinet manufacturers. These cabinets must include ventilation, power, rack, and noise cancellation technologies.

PLANNING CHECKLIST

- 1 List the server room factors to consider when choosing a site.
- 2 Choose the site.
- 3 Define the equipment to be installed, including power, air conditioning and air filtration.
- 4 Determine how you will secure access to the room, such as electronic badges with a logging system.
- 5 Create an implementation plan, approve budgets, choose suppliers and sign contractual agreements.
- 6 Ensure that work is completed on schedule and to appropriate standards.
- 7 Create an installation plan for server room equipment.
- 8 Have equipment delivered and installed.
- 9 Qualify the room and equipment before starting operation.
- 10 Set up a formal review process to periodically check on-site operation.

CONTACT INFORMATION

LAD ENTERPRIZES, INC. www.ladenterprizes.com
David Burford dave@ladenterprizes.com 610-429-3122