BLACK BOX®
NETWORK SERVICES

Power Protection

**Understanding the
risks to your network
and how to choose
the right solution.**

Table of Contents

We're here to help! If you have any questions about your application, our products, or this white paper, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box." You'll be live with one of our technical experts in less than 30 seconds.

Introduction

Your company, like many others, has a sizable investment in computer networks: hardware, software, and customer-related information. You also have a significant investment in the people and processes that support the mission-critical applications you depend on daily to run your business. But one electrical anomaly—one good zap to your network—can sideline this entire segment of your company's operation.

Computer networks are electrical systems. Network devices rely on steady, even power— as Goldilocks would say, "not too much, not too little, but just right."

Power fluctuations can wreak havoc with a network. In a worst-case scenario, power or surge-related problems affecting servers, routers, or switches can bring your business to a halt. And with the growing demand for interconnected computer, telephone, and LAN systems, many new pathways for power, surge, and transient problems are created every day. That's why your computer network requires complete protection on all AC power and datacomm lines.

Assess your own situation. We think you'll see that prudent investment in thorough protection is minor compared to the costs of repairing or replacing damaged components. In fact, compared to the crippling costs of lost productivity, idle employees, lost opportunity, and unhappy customers, you'll probably find the costs of protection inconsequential—if you take action now.

Power Lines

Network power protection means ensuring that your electrical lines always supply a steady, uninterrupted supply of power free from damaging electrical fluctuations and that your data lines are always protected from electrical interference and ground loops. It also means providing protection against the devastating damage of a lightning strike.

Like so many operations connected to your network, power protection is largely a matter of common sense and proper planning.

Catastrophic and disruptive power conditions

Millions of desktop microcomputers, printers, and other peripherals are typically powered from standard AC wall outlets. And that means they're susceptible to all the variations in the public power supply. Plus, your own building may contain machinery that can adversely affect the quality of your power.

How can you tell when your computer system is suffering from power problems? Look for these symptoms:

- Damaged hardware
- Overall system slowdown
- Numerous service calls
- Damaged or lost data or software
- Erratic operation
- Failed tests and system lockups
- Unexplained problems
- Numerous service calls but no problems found
- Unreliable data

Power losses

Sags and brownouts are a short-lived decrease in line voltage. Sags are generated by the startup electrical demands of devices like motors, compressors, elevators, copiers, and air conditioners. Sags may also occur when the utility company systematically lowers voltage levels to meet extraordinary power demands (Figure 1).
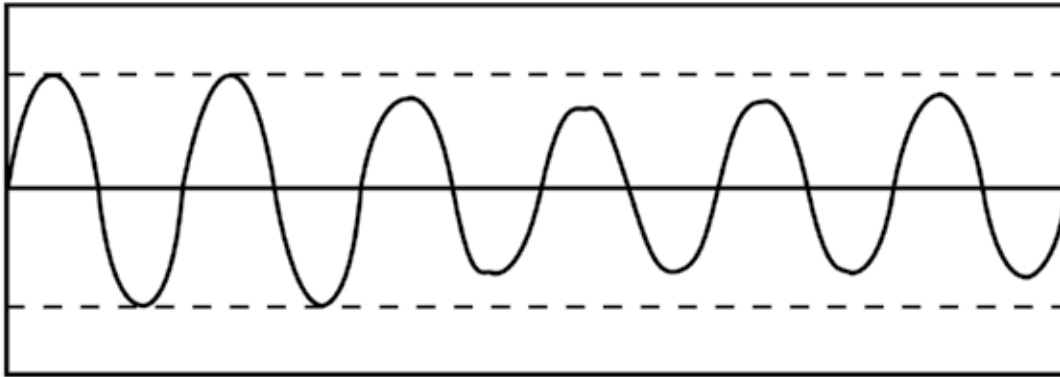

Figure 1: Power sags are short-term decreases in normal voltage levels.

Brownouts are long-term undervoltage conditions that are actually planned by electric utilities or are the result of excessive loading. There are many locations throughout the United States that experience chronic brownout conditions. Typically, these are caused by the seasonal demands of air conditioners or by heavy loading during peak usage times of the day.

A blackout is a total power outage that results from excessive demand or catastrophic incidents such as lightning, ice storms, car accidents, or natural disasters. A blackout brings your system to an instant halt.

Power impulses

Impulses are indicated by a sharp, instantaneous rise in voltage and are typically caused by damage from storms or lightning. Electrical impulses are particularly destructive and can damage or destroy electrical equipment instantly.

An impulse can be additive (a spike) or subtractive (a notch) and may oscillate back to within normal voltage levels (Figure 2). A total, brief loss of power is a kind of impulse known as a dropout. Dropouts can last from one millisecond to a full second and are usually caused when the electric company switches power grids.

Sometimes, electrical impulses are inaccurately referred to as transients, a term that reflects their erratic nature.
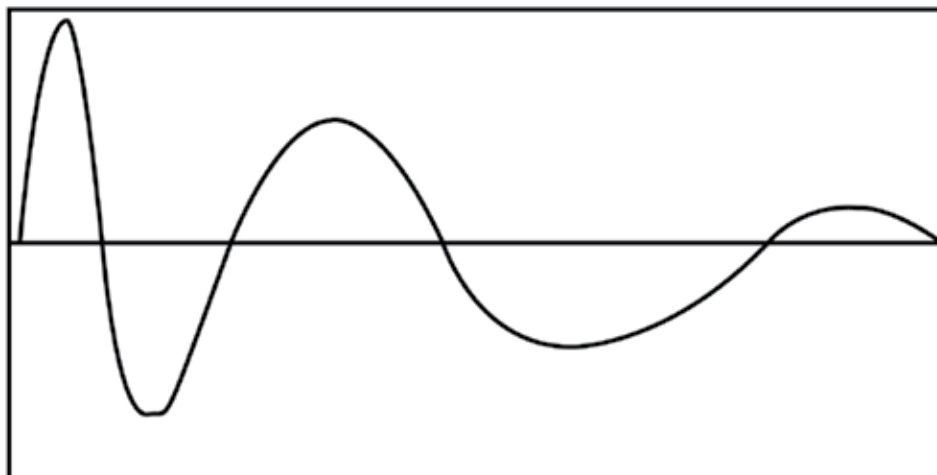

Figure 2: The effects of various impulses on a sine wave.

Power surges

A surge is a brief rise in voltage that's caused when power is switched on or off to a high-powered motor or a solid-state device like an industrial drive system. Note that a surge is not the same as an electrical impulse or a spike; instead it's an intermittent condition that occurs when a series of peak sine-wave voltages exceeds the standard voltage level for a sustained period of time—anywhere from eight milliseconds to two and a half seconds (Figure 3). Surges stress electronic components by exceeding their specified voltage ranges. This can significantly reduce the reliability and life expectancy of any electronic device.

Other power disturbances are overvoltages and undervoltages. These refer to conditions, like sags or surges, that last longer than a few seconds.
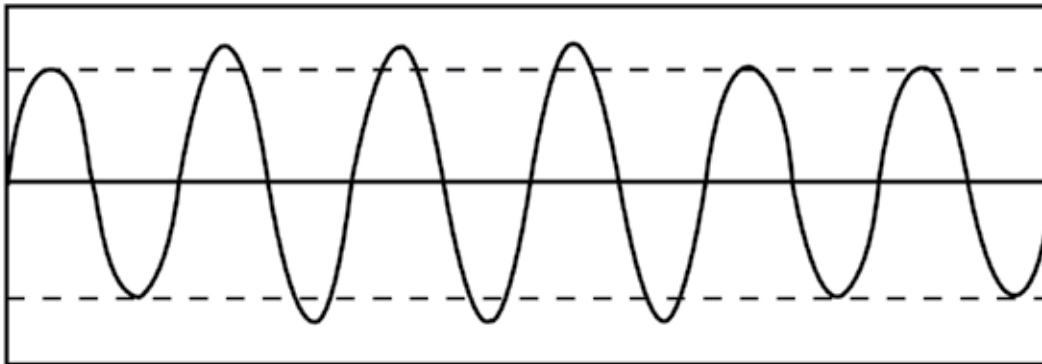
Figure 3: Surges are short-term disturbances that exceed normal line-voltage limits.

Electrical noise

If you've ever listened to an AM radio or tried to watch television while someone was running a vacuum cleaner or using a blender, you've probably heard the high-pitched whine or seen the on-screen static caused by electronic noise. That "noise" is actually electromagnetic interference (EMI). It's conducted from the spinning appliance motor onto the AC power line and output through the TV or radio along with the normal audio or video signal.

Radio-frequency interference (RFI) can also disrupt the power signal to your computer or any other nearby electronic device. In fact, noise is defined as any electronic signal that's present on an AC power line in addition to the desired signal. It can range in intensity from low-level disturbances to large transients with damaging impulses, or it can be a continuously oscillating signal from a nearby motor or some other source.

Protecting your network from disruptive power conditions

Today's advanced computer equipment requires a steady, uninterrupted supply of 120 volts alternating current (VAC). In the U.S., this is the standard power provided to most homes and businesses by local public utilities. This electricity is generally affordable, clean, and reliable, but it is subject to fluctuations.

Surge protectors

There are many different kinds of surge protectors. Practically speaking, surge protectors installed on power lines don't absorb or otherwise diminish damaging power surges. Their primary function is to divert these destructive forces away from your sensitive circuitry. There are four basic kinds of surge protectors: metal oxide varistors (MOVs), avalanche diodes, filters, and gas tubes.

Metal oxide varistors (MOVs) are a common choice. The word *varistor* is a combination of two words: variable resistor. As these words imply, an MOV is a highly resistive device that triggers during an AC power surge and diverts the excess voltage, preventing it from reaching your expensive computer equipment.

MOVs are designed to accommodate surge levels up to a specified breakdown voltage. When this limit is exceeded, the MOV varies from a highly resistive state to a state of low resistance. The excess energy is "clipped' from the power line and sent to ground.

Surges occurring at the peak of a sine wave are clipped by the MOV, but note how MOVs function during a negative-peak surge (Figure 4). High-voltage spikes may still occur (though they'll eventually be clipped), and the MOV response times can range up to 500 picoseconds. This is the primary weakness of an MOV, but it's usually overcome by the inclusion of some other suppression technique within the surge protector.
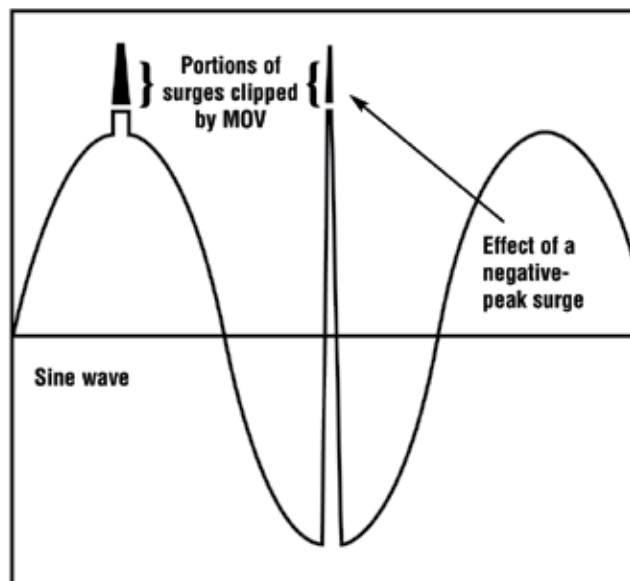

Figure 4: Sine wave showing surges and how they're clipped by
metal-oxide varistors (MOV).

Avalanche diodes, also known as Zener diodes, are semiconductor devices similar to MOVs, but they feature much faster response times (usually less than one picosecond). Avalanche diodes are available in a wide range of sizes to provide accurate and repeatable voltage clamping.

However, they have a limited ability to withstand large surges, which means they should be combined with other devices to make them useful for lightning surge protection. Filters are also usually built into surge protectors, along with other suppression devices, to offer enhanced levels of protection. They're made up of discrete coils, called chokes, and capacitors that are designed to filter noise occurring within specific frequency ranges on AC power lines (Figure 5).
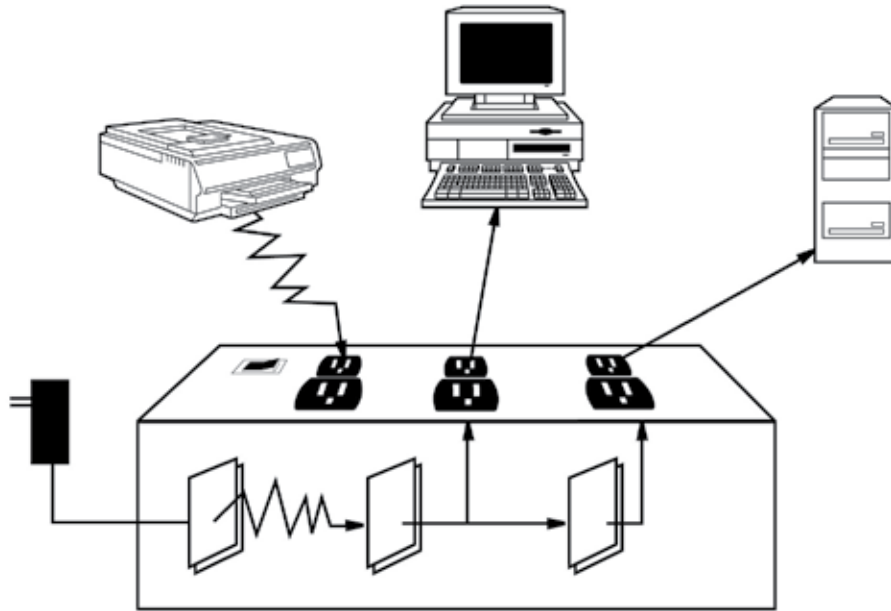

Figure 5: Noise filters prevent AC-surge and line-noise contamination.

Gas discharge tubes are specialty devices usually installed near a building's main service entrance or transformer to divert particularly devastating surges well before they enter your building. Intense voltage levels striking the tube ionize the gas, turning it into a conductive path to ground. Gas discharge tubes generate their own disruptive high-frequency levels during this grounding process, so they should never be installed near any electronic equipment that might be damaged as a result.

Gas tubes can absorb huge voltages, so they're often used to protect against lightning strikes. However, they take a certain amount of time to activate—just enough time to let in a surge that can fry solid-state computer equipment. For this reason, they're best used with other forms of surge protection.

Because all the common surge protection methods have inherent advantages and disadvantages, the best systems use more than one type of component to achieve the best performance. These combinations of surge protection methods are generally known as multistage hybrid circuits. The most common combinations incorporate a high-current but relatively slow-acting component with a faster-acting but lower-power-rated component.

Choosing surge protectors

A good surge-protection system involves more than one type of protection—silicon avalanche diodes for quick response, for example, with gas tubes to take the main hit. When evaluating surge protectors, you should also look at the clamping voltage, UL® clamping category, and the maximum surge current.

Clamping voltage is a measure of the actual voltage level that the protective device will allow through to your equipment. Often called the let-through voltage, this measure is the best performance indicator to consider when choosing surge protection equipment. The lower the number, the better the degree of protection.

UL® clamping category is a rating of surge protector effectiveness defined by Underwriters Laboratories®. As with clamping voltage, the lower the number of the UL® clamping category, the better protection you can expect for your equipment. However, note that devices rated within a similar category may have a wide range of clamping voltages.

Maximum surge current is a measure of overall capacity for diverting surges or the highest voltage a surge protector will take before "sacrificing" itself. In the face of an extremely large surge, a surge protector will break the link to your hardware and sacrifice itself. Ultimately, surge protectors are designed to fail.

Uninterruptible power supplies (UPSs) and backup power supplies (BPSs)

Most power problems are brownouts (low voltage) or blackouts (complete outages). Only an uninterruptible power supply (UPS) or a backup power supply (BPS) can protect your systems against conditions of too little power.

For a small fraction of the cost of your networking hardware, you can purchase a UPS or BPS that protects your network from brownouts, blackouts, and surges.

To prevent power disasters before they happen, more than 70% of servers are protected with a UPS or BPS. Network managers know that having a server down brings many operations to a halt. Although the loss of a single hub or router may not bring the entire corporation to a standstill, it can result in zero productivity for entire workgroups or remote offices.

A UPS or BPS keeps power flowing, giving you enough time to shut down safely during a power outage. It also regulates your power, smoothing out dangerous overvoltages and undervoltages, spikes, surges, and impulses that often go unnoticed.

The difference between a UPS and a BPS is that a UPS provides continuous power that stays up during a power outage whereas a BPS provides standby battery backup to which it switches during a power problem.

With a UPS, your equipment is always running on battery power, which is continuously being recharged from your regular power lines. Because there is no switchover time with a UPS, it's a particularly stable source of power. Continuous UPSs, although they can cost twice as much as a standby BPS, provide extremely stable power and are frequently used in server rooms and other critical network applications.

A BPS does not operate until it detects a problem. If the power goes out or sags, it switches your equipment to battery power very quickly. Even though this switchover is nearly instantaneous, there is a small lag, which may affect your equipment. BPS systems cost less than UPSs and are commonly used in home or small business networks and for desktop computers.

Note that neither UPSs nor BPSs are standalone power generators designed to deliver a continuous supply of electricity. They're backup systems built to provide specific levels of emergency power for a limited amount of time, called the run time. You can extend the run time by adding battery packs, but the duration of any backup device's run time depends on the power load drawn by all the attached devices.

Most UPS or BPS systems today also provide sophisticated protection from surges and other overvoltages, and filter out line noise. Many log power problems, enabling you to keep a close eye on power conditions within your network. A properly installed UPS or BPS can be all the power protection a small network needs.

Choosing a UPS or BPS

There are systems available to support almost any equipment for time intervals of anywhere from five minutes to two days. You should plan on at least enough run time to allow you to save any open files and safely shut down the system.

A quick way of estimating how much backup power you'll need is:

1. List all the equipment you have that needs protection. Remember to include monitors, terminals, hard drives, external modems, and any other equipment in the critical path of potential power or surge sources.

2. Add up the total amperage ratings of your equipment. This information is often imprinted on the back of each device.

3. Multiply this total amperage figure by the operating voltage (typically 120 VAC in the U.S.) to obtain your total volt/amp (VA) requirement with a safety margin.

4. Select a UPS or BPS with a VA capacity at least as high as the amount in Step 3. To accommodate future expansion, it's wise to order a device with an even larger VA rating.

For large networks and very complex installations, call in a professional. In the long run, an expert will save you money by fitting a UPS or BPS system precisely to your application.

Grounding

Grounding protects your network from unexpected power surges—especially those caused by nearby lightning strikes—by conducting surges of negatively charged electrons to the positively charged earth. Your objective is to make sure that the negative charge gets safely to ground without going through your network along the way. This calls for proper grounding to dissipate overvoltage—potentially at high current—very quickly and for proper surge protectors that divert large surges to ground.

Proper grounding is an art form—to be effective, the common earth ground must be the best ground in the building. A metal rod sunk into the earth is often used as a ground. Many newer commercial construction uses the building's steel as an earth ground, which is an excellent method.

The problem is that sometimes another building feature such as the plumbing can provide a better ground than the intended ground. When electrical surges use this unintended ground, they may travel through sensitive equipment along the way.

Tips for proper grounding:

1. Whenever possible, connect devices to a single ground point.

2. Equalize the potential differences between hardware chassis through single-point grounding. We recommend using a power strip or supplemental ground strips between each chassis.

3. Keep ground connections as short as possible to ensure a low-impedance path to ground.

4. Make sure the neutral-to-ground bonding point is as close as possible to the computer.

5. Use large conductors for green-wire grounds to ensure a low lead impedance. Don't use conduit as a ground path because it can easily come loose or corrode over time.

Data Lines

Data is transmitted across copper lines using electrical impulses, too. Unexpected electrical interference on these lines can interrupt the smooth operation of your network.

Surges

Power lines aren't the only way surges can get to your equipment. Any communications line can also be a source of damaging surges. These surges can come in from the outside through telecommunications lines. However, many surges that are assumed to originate in phone or other telecommunications lines actually enter on power lines and find a ground in the phone line.

Data line surges can also originate in your own equipment. This is because most networking devices are connected to both a power line and a data line. If the data ground is "better" than the power ground—for instance if it's plugged into an ungrounded outlet—then any electrical system surge will go through the equipment circuitry and out the data ground, often traveling across data lines into other equipment to do so. Data line surges often damage equipment that was thought to have been already protected because it had surge protectors on the power lines. Network interface cards are particularly vulnerable and can be destroyed by relatively mild electrical spikes.

EMI/RFI

Electromagnetic interference (EMI) and radio-frequency interference (RFI) can interfere with data transmission over copper wires, slowing data flow and causing errors. Although EMI/RFI often comes in over your equipment's power lines, it can also affect data lines directly when your network cabling is installed near sources of interference such as fluorescent lights or elevator motors.

Ground loops

An electrical problem not often thought about or understood is that of ground loops, which are often encountered when running copper data lines between two buildings although they can occur within the same building as well.

When a copper cable links devices that draw power from separate electrical sources with different grounding systems, ground loops can happen. Although each device references its own grounding system as zero volts, differences in the earth's composition at the separate grounding sites may actually yield a voltage difference higher or lower than zero when the systems are compared to one another. If there is a difference, a ground loop is created when the two devices are connected, and the excess energy causes the data line voltage to fluctuate as information is transmitted in both directions.

Unlike electrical surges, which are fast-rising voltage spikes that last a very short time, a ground loop is a constant electrical state that can, over time, cause equipment malfunctions or even severe damage. It's tough to diagnose ground loops, but unexplained system damage such as strange outages and failing components are all common symptoms of the problem. Fortunately, ground loops can be easily prevented.

Solutions for data-line electrical problems

Fiber optic cable

Fiber optic cable is the ideal choice for installations between buildings because it doesn't carry electrical surges caused by nearby lightning strikes or cause ground loops. All your data line surge, interference, and ground loop problems can be solved simply by installing fiber optic rather than copper cable. Common copper cable works by carrying electrical impulses. The problem is that any other kind of electrical impulse can also travel along the copper cable, too. On the other hand, fiber optic cable is completely immune to interference. The fiber is made of glass, which is an insulator, so no electric current can flow through.

There are other reasons to choose fiber optic cable as well: Fiber offers greater bandwidth than copper and can operate over longer distances. With all these benefits and with the cost of fiber installation dropping, fiber optic cable is rapidly becoming a top choice for new cable installations.

If you have existing copper cabling, fiber optic cable can be used to create surge-proof "firewalls" within your network.

Copper cable solutions

One basic precaution for copper cable is to avoid running it in electrically noisy areas such as near heavy machinery. If you must run copper cable through an electrically noisy area, choose a shielded cable. Foil is the most basic cable shield; a copper-braid shield provides even more protection.

There are two primary options to protect data lines from surges: grounded surge protectors and opto-isolation.

Grounded surge protectors—usually with avalanche-diode technology—divert excess energy to an earth ground. They're simple to install: Just connect them between ports and data lines then connect the ground. That little pigtail of a ground wire hanging off the surge protector is very important. It needs to be connected to ground for the surge protector to work. If you install the surge protector but don't connect the ground, you might as well not install a surge protector.

Opto-isolators use fiber optic technology to effectively break the pathway over which potentially damaging ground loops can travel between separate electrical systems. These devices contain photoelectric transistors that introduce a physical gap in the circuit. The transistors convert digital electrical signals from copper wires into light pulses that are transmitted optically across this gap—literally through thin air—interrupting the copper-wire connection. This enables you to use your existing copper wire without worrying about ground loops.

There are a variety of opto-isolators to choose from, so select one that's appropriate for your system. Just one standalone unit can provide protection for an entire between-building network. You'll find other types of opto-isolators integrated into devices such as line drivers and interface converters. Many surge protectors feature built-in opto-isolators, but if you use these in a building-to-building network, you need to install one at each site. That's because even though one opto-isolator is all it takes to prevent ground loops, you still need dedicated surge protection at each end of the circuit to prevent damaging surges and spikes from entering either building over the outdoor cable.

If you've already installed copper cable between buildings and decided that replacing it with fiber optic cable is cost prohibitive, opto-isolation is an inexpensive cure for ground loops.

Static electricity

We've all felt the subtle sting of a static electric shock—that tiny spark that arcs from your fingertips to a metal doorknob after you've walked across a carpeted surface. But did you know that a single electrostatic discharge packs enough energy to erase portions of an EPROM chip or corrupt data on a diskette?

Static electricity is a charge that builds up when two dissimilar objects rub against one another—like fabric in a clothes dryer or shoes on a carpet. Under normal conditions, this charge dissipates gradually through conduction with the moisture in the air around us. But when the air is particularly dry, such as during wintertime, there's less humidity so the air becomes much less conductive. This provides an opportunity for electrostatic charges to accumulate quite a large potential, which, if discharged by touching sensitive electronic devices, may be destructive.

You can take precautions to avoid the threat of static discharges by using special static-free floor mats in your work area and by humidifying the air in your building during heating season.

Lightning and lightning rods

You may have noticed that all our previous discussions of lightning specified "nearby" lightning strikes. Although surge protectors and grounding can shield your network from power surges caused by lightning nearby, they cannot protect your systems from a direct hit by lightning. A direct lightning strike is a devastating electrical event that can cause as much as two billion volts at 500,000 amps to slam into your network all at once. The large electrical charge field of a direct lightning strike causes a massive surge that travels through the air, along walls, through anything in its way, bypassing surge protection and frying anything that it touches. It will damage equipment that is powered off or even unplugged. Nothing is safe from a direct lightning strike.

Lightning is one of the most destructive forces on earth. The federal government says that lightning strikes cause billions of dollars in equipment and facilities damage each year. The Lightning Safety Institute reports that lightning causes more than $5 billion in annual property damage in the United States alone. And that's just equipment—it doesn't count the cost of down-time and lost data.

Although surge protection offers little protection from direct lightning strikes, you can actually prevent most lightning strikes through the use of proper lightning protection: lightning rods.

Lightning rods do not, as is widely believed, attract lightning and conduct it safely to the ground. Their job is to prevent lightning from striking your building by encouraging it to strike somewhere else. Here's how lightning happens and how lightning rods work:

The earth has an extremely large positive charge caused by ionization of iron and silicon deep within the mantle. A lightning strike occurs when a negative charge builds up in the bottom part of the cloud closest to the earth and a positive charge of energy accumulates directly underneath in the ground. As the two opposite charges build up, eventually the negatively charged electrons start down toward earth. At the same time, the positive ground charge is attracted upward. This massive exchange of electrical energy is what causes lightning. And lightning discharges through whatever happens to be in its way —your building, your network, or you!

When a negatively charged storm cloud travels across the countryside, it drags a positive charge along beneath it across the surface of the earth. When the cloud travels above a tall structure, such as a building, an antenna, or a tree, the attraction of the negative cloud charge pulls the positive ground charge up into the top of the structure, and concentrates the ground charge there. This makes this high structure more likely to be the object of a lightning strike than the surrounding countryside.

A lightning-rod system protects a structure by providing lots of high points for the positive charge to accumulate at. Because the positive charge is spread around, it's not as strong and this reduces the possibility of a lightning strike. Lightning rods do not reduce this charge accumulation very much—but they only have to reduce it by a very small percentage to encourage lightning to strike an accumulation of positive charge elsewhere. It's important to have your lightning-rod system installed by professionals who know exactly what they're doing. "Lightning-rod salesman" used to be a generic term for a traveling con man—and with good reason. Improperly installed lightning rods can make lightning more likely to strike, not less. Leave the installation to the experts.

Disaster recovery

Even the best protection only lowers the odds of having your system go down—your network can still be demolished by one direct lightning strike, the power could go out for a week but your UPSs only provide backup power for an hour, or you could even be hit by a non-power-related emergency such as a flood or an earthquake. There is no such thing as 100% protection from network disaster, so be prepared to act if the worst should happen.

System backup

One of the most effective methods of preventing data loss is to back up your data regularly. The usual system for networks is to back up network servers nightly onto high-capacity tape, copies of which are then rotated into an off-site storage facility. You should always store copies of your backups off-site. There are many companies that provide secure, climate-controlled storage service, as well as pickup and delivery.

Replacements

Prepare a detailed inventory of all your network components and make sure you keep it up-to-date. The inventory should cover all hardware, software, communications equipment, peripherals, backup media, and power-conditioning equipment. Include model and serial numbers of all components. Now, make a plan to replace all these components quickly in case of disaster. Make sure that you not only have the name of a vendor handy, but also the name of an alternate vendor. Consider negotiating a standby agreement with a local vendor for priority replacement of LAN components in case of an emergency or a disaster.

Insurance

Buy good insurance with adequate coverage for all your LAN equipment. You need to be ready to replace any components that get lost in a disaster, and being ready means having the money to do it—that means good insurance so you don't get stuck with the bill.

It's especially important to make sure that your insurance policy covers natural disasters such as lightning strikes. If your policy has an "acts of God" exemption that won't cover natural disasters, it's worth paying to upgrade your protection.

Conclusion

Complete network power protection requires a unified plan. You can't just throw in a few surge protectors, a UPS, and a length of fiber optic cable and expect adequate protection.

Power protection in small networks can easily be planned and managed by the average network administrator. Install properly sized UPSs between your equipment and your electrical service, put grounded surge protectors on all incoming data lines, have a good backup plan, and your network is covered.

However, for large networks—especially networks spanning multiple sites—you will get the best, most cost-effective power protection by consulting an expert cable installer with experience in installing surge protection. An expert can factor in such diverse elements as your building's metal frame and how lightning-prone your area is, to come up with the most effective power-protection plan for your particular situation.

About Black Box

Black Box Network Services is a leading technology product solutions provider, serving 175,000 clients in 141 countries with 198 offices throughout the world. The Black Box catalog and Web site offer an extensive range of products including Outlet-Managed PDUs, Elite™ Managed Power Controllers, Opto-Isolators, and surge protectors.

Black Box also offers cables, testers and tools, cabinets and racks, remote monitoring and security, KVM, digital signage and multimedia, and networking solutions.