Ground Potentials and Damage To LAN Equipment

KEVIN KANAKOS
Peradata Technology Corporation

INTRODUCTION

Many companies turn to local area networks (LANs) as a means to automate their data processing operations. Network data cables encompass entire buildings and also span buildings and campuses. LANs have become an interconnection of computers, building power systems, telephone, data acquisition, and video and security systems.

As LANs become larger, LAN equipment becomes more vulnerable to damage from voltage surges that appear on network cables. The reason for this vulnerability is that LAN data cables also interconnect the grounding systems of what are, in some cases, separate electrical power systems. A *ground potential difference* occurs when "ground" in one part of a building is at a different voltage than "ground" in the rest of the building or in a neighboring building. Data errors often occur when a ground potential difference exists between network devices. The results are more dramatic when network cables span buildings.

With advances in LAN technology, many companies have shifted critical operations and data to file servers on a network. LAN managers have learned the hard way how fragile and vulnerable their networks can be to AC power dropouts, voltage fluctuations (brownouts), and AC power surges. As a result, the need for uninterruptible power supplies (UPS) and ac power surge protection has become well-accepted.

Aside from the ac power plug, all LAN devices have one other common connection – the network data cable. By design, signals on network cables reach every device on the network. Damaging surge voltages travel just as easily throughout the network. Computer and communication integrated circuits have become denser and faster by reducing their internal circuit spacing. As a result, they are less able to withstand overvoltage stress and are easily damaged.

Network data cables form redundant ground paths with the electrical wiring of a building, leading to undesired signals and surges on data cables during lightning strikes and power line disturbances.

THE ROLE OF GROUND

The building ground system is provided primarily for electrical safety. A lethal condition occurs when an electrical fault in a piece of equipment puts line voltage on a touchable surface of the equipment. The internal connection of the equipment chassis and ground conductor of the ac power plug causes the fault voltage to "short" to ground rather than energize the equipment chassis. The fault current flows from the equipment's receptacle ground through the building wiring to the ground at the service entrance. There, the neutral and ground conductors are connected. The fault current trips the branch circuit protector (fuse or circuit breaker) and removes the dangerous condition. The National Electrical Code (NEC) contains many requirements that must be followed so the electrical system of a building can provide this protection.

The building ground system also plays a role in lightning protection. When lightning strikes nearby power lines, large currents will enter the building's electrical wiring and flow through the ground conductors. If lightning strikes the building itself, the current will flow through all parts of the building. This includes the structural steel and the power lines, conduit and raceways that connect to it.

Apart from the safety aspects of poor grounding, a poor ground system can wreak havoc with a LAN. Poor grounding can be attributed to incorrect wiring or installation and damaged connections due to vibration and corrosion.

The building ground system also provides, ideally, a voltage reference point, 0 V, for all equipment connected to the electrical system. Data communication circuits use this ground reference to measure the relative signal levels of the data when it is received. When ground is at 0 V throughout the LAN cable system, network data can be received and interpreted properly by each device on the network.

In the real world, however, the potential of the ground at each point in a building, is determined by the amount of current flowing through the ground conductor multiplied by the impedance of the ground system (Ohm's law). The impedance of the ground system includes the resistance of the ground conductors, connections and splices from the ac receptacle to the final connection to earth ground. During a transient event, such as a lightning strike or power line surge, the inductance of the ground wiring significantly limits the effectiveness of the ground path in protecting sensitive digital circuits.

GROUND POTENTIAL RISE

Consider the case where a workstation in Building A is sending data to another network device in Building B (Figure 1). The ground potential of each building will be a function of the impedance of its ground system and the current flowing through the ground. The data line, in addition to carrying data, is also connecting together the ground systems of the two buildings. If the ground potentials of Building A and Building B are different, a ground current flows in the data line. This is known as a *ground potential difference.* The voltage level of the data signals is increased or decreased by the ground potential difference, causing data transmission errors.

It is not unusual for a nominal, *steady-state* ground potential difference to exist between two buildings. There are cases where the potential difference has burned open data cables because of the current flowing from one building ground to another. This usually indicates an electrical equipment fault or incorrect building wiring. Weather conditions such as rain can affect ground potential differences. The water-saturated soil is better able to carry current to earth ground. Note that the improved ground conductivity can either improve or worsen the potential difference problem. Under normal conditions there should be very little current flowing in the ground conductor.

GROUND POTENTIAL TRANSIENTS

Transient events are a much greater source of ground potential differences. Lightning strikes are the most obvious source and often involve the building ground system. During a strike, instantaneous currents of 100,000 A are possible. If the strike occurs near Building A, as in the example above, some of this current flows through its ground system on its way to earth ground. Besides the damage done in Building A, the high current impulse will cause an instantaneous rise in the Building A ground potential. For example, a 10,000-A lightning current flowing through the building's (ideally) 0.1- ohm ground impedance creates a 1000-V transient rise in the ground potential of Building A. The potential difference of the two buildings' grounds causes current to flow through any electrical path between the two buildings. In this case, a transient surge appears on the network cable connecting it to Building B. This transient surge can last for several microseconds. Any unprotected LAN equipment connected to the network cable in Building B will be damaged (Figure 2).

An unexpected source of transient ground potentials is the surge suppressor protecting the ac power for the network equipment. With few exceptions, ac surge suppressors protect equipment from power

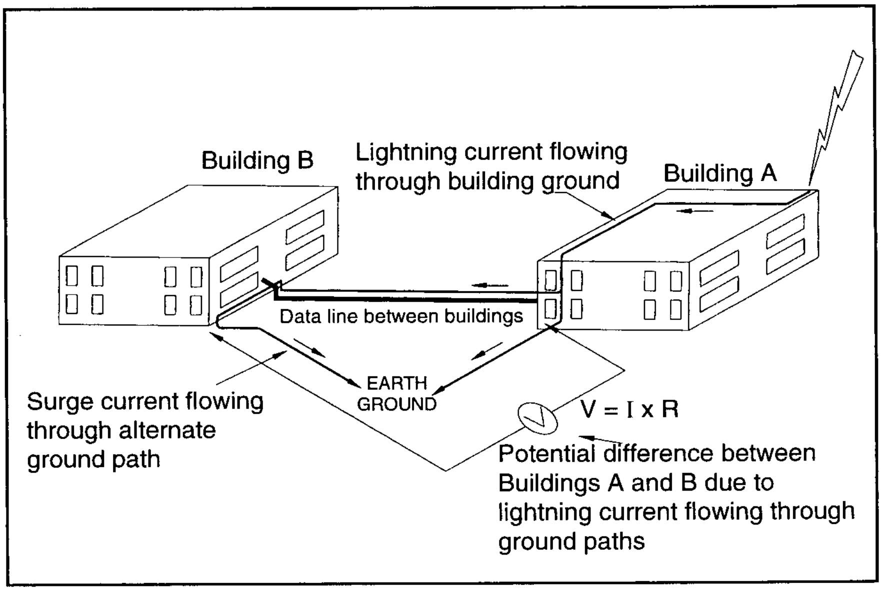

Figure 1. *Ground System of LAN.*

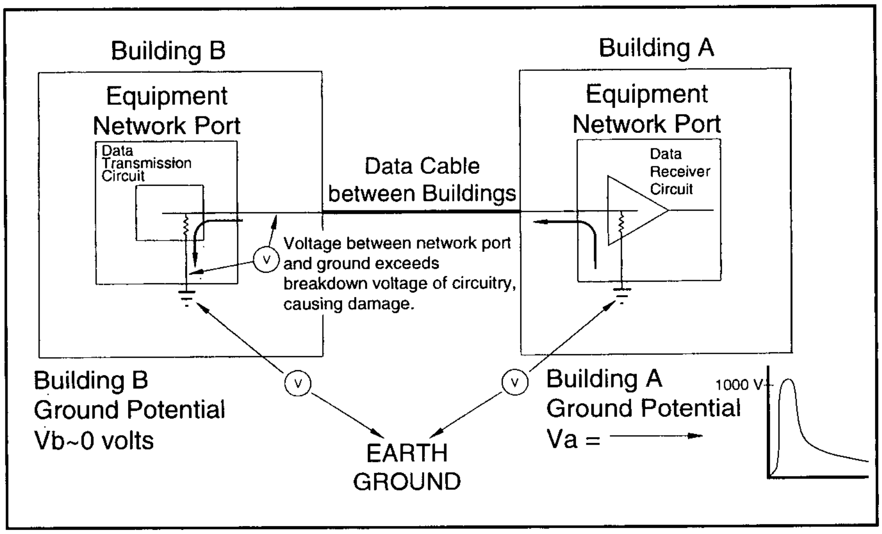

Figure 2. *Voltage Surge as it Affects LAN Equipment.*

surges by diverting the surge energy into the ground system. Indeed, the standards used for certifying suppressors encourage this design. Surge suppressor performance is measured by how well the surge is diverted into the ground system, without limiting the large current transient that causes ground potential rise. There are "series mode" ac power surge suppressors available which work by spreading out the surge over time so the ground system can absorb the current slowly, without creating a ground potential rise. Their added cost is more than justified by their superior performance.

The problems which affect connected equipment in different buildings also cause damage to LAN equipment located within the same building. Once again, the integrity of the grounding system can determine whether or not equipment damage results. During a transient event, a potential difference can exist between the ground conductors of different parts of the same building. As the potential difference equalizes throughout the ground system, it creates a transient surge on the LAN cables. The result is damaged network cards, blown ports on a hub, etc.

PREVENTING DAMAGE TO NETWORK EQUIPMENT

There are two remedies that reduce the threat of network equipment damage from data line surges: data line isolation and data line surge suppression.

When a steady-state potential difference exists between two ground points, it is sometimes possible to identify the cause. It may be that part of the building wiring or a piece of equipment is incorrectly installed. Poor ground connections in the receptacle, splices, or at the service entrance panel can create a high impedance ground path. These should always be remedied because of the safety aspects. Consultants can be contracted to diagnose the building's electrical and interference problems and to recommend solutions.

Inevitably there are situations where the ground potential difference between two network devices cannot be resolved. One solution is to break the copper data line connecting the two network devices. Installing a fiber optic link in place of copper is an effective but costly solution. Data line isolator units, which connect in series with the data line, can also be used. These units break the electrical connection between two data ports but allow data to pass between them.

Data line surge suppressors operate by "clamping" the data line to ground whenever the voltage exceeds a certain level. After the transient surge has passed, the suppressor "turns off," allowing normal data traffic to resume. Data line surge suppressors should be connected right at the network port of the equipment being protected. The suppressor ground strap should be connected only to the equipment chassis. This ensures that there is no potential difference between the suppressor ground and the equipment ground when a transient surge is being suppressed. For this reason, data line surge suppressors that connect to ground at the receptacle are not as effective. When installing data line surge suppressors, they should be used in pairs to protect the equipment at each end of the cable.

Several misconceptions persist about how to use data line surge suppressors. Ironically, some of these originate with manufacturers.

- Data line surge suppressors do not prevent noise from interfering with or corrupting data. If the voltage on the data cable is high enough to "trip" the suppressor, then the data is already corrupt.
- Surge suppressors do not prevent ground loops from corrupting data for the same reason.
- Data line surge suppressors are the wrong choice when a steady-state ground potential difference exists. If the ground voltage exceeds the suppressor "trip" voltage, the data line will be continuously clamped to ground. If the ground voltage is high enough, the continuous current diverted to ground will burn open the suppressor. A properly designed suppressor will interrupt the data flow when its circuits become damaged. In any event, using a surge suppressor in this application will not restore data transmission. Isolation is a better solution.

AC power surge suppression should be installed as close to the service entrance as possible where the impedance to earth ground is lowest. If installing individual ac power surge suppressors for network equipment (still a good idea), the higher quality series mode suppressors that do not create high ground currents during operation should be considered. If a particular piece of equipment (e.g., a large motor) is causing the problem, wiring it to a separate ac circuit is recommended.

CONCLUSION

With the increasing size of local area networks, the network data cables form redundant ground paths with the electrical wiring of a building. This inevitably leads to undesired signals and surges on data cables from lightning and power line disturbances. Proper grounding methods and compliance with the NEC are essential to minimize surge damage to network equipment. To protect network equipment from damage, surge suppressors should be installed at the network ports of the equipment or isolators can be used to break the copper path that carries the surge current.

***KEVIN KANAKOS** is president and founder of Peradata Technology Corporation, a manufacturer of data communication equipment specializing in line isolation and surge suppression systems. Mr. Kanakos received his bachelor's degree in electrical engineering from Manhattan College and a master's degree in industrial management from Polytechnic Institute of New York. He founded Peradata Technology in 1985. (516) 588-2216.*