

Lightning Surge Damage to Ethernet and POTS Ports Connected to Inside Wiring

Joseph Randolph, *Member, IEEE*
Randolph Telecom, Inc.
Winchester, Massachusetts USA

Abstract - In recent years, many suppliers of telecom equipment have reported higher than expected rates of lightning damage to Ethernet and POTS ports connected to cables located entirely within the same building.

There are three known mechanisms by which lightning surges can be coupled onto inside wiring, but these mechanisms are statistically infrequent. Given the reported rates of surge damage, these known mechanisms do not provide a simple explanation. It appears that additional surge coupling mechanisms may be involved.

The three known mechanisms are described, and it is shown that surge damage from these mechanisms should be infrequent. Three new theories for additional coupling mechanisms are then described. All three of these new theories are based on the notion that surges appearing on the AC mains outlets in the building are being coupled onto inside wiring communication cables.

The analysis suggests that the first of these additional coupling mechanisms seems an unlikely cause for the apparent increase in surge failures. The second mechanism appears more plausible, particularly because it correlates to the recent industry trend of implementing wall mount Class II AC mains power supplies as switching converters rather than traditional linear supplies. However, the theory behind this second mechanism only applies to surge failures of Ethernet ports.

A third potential mechanism is based on unintended side effects of consumer grade multi-port surge protectors used in installations with poor grounding. This mechanism applies to both Ethernet and POTS failures.

Further study will be necessary to determine whether any of the three additional mechanisms are in fact the cause of the apparent increase in field failures. In the meantime, some guidelines are presented for manufacturers who wish to implement enhanced surge protection on Ethernet and POTS ports that connect to inside wiring.

I. INTRODUCTION

The traditional view of lightning risks for wireline communication cables has focused on cables that are strung

outside, such as on telephone poles or other exposed environments. In general, cables that are routed entirely within a building have been regarded as inherently protected from lightning surges.

Lightning protection engineers have always understood that this view is not strictly correct. There are known mechanisms by which a nearby lightning strike can induce surges on inside cables. However, the known mechanisms generally come into play only when lightning strikes an object close to the building containing the inside cables, or strikes the external envelope of the building itself. Such events are comparatively rare.

In recent years, higher than expected surge failure rates have been reported for ports connected to inside cables. It is possible that the apparent increase is simply due to the fact that more inside wiring ports are being deployed, causing the conventional surge mechanisms that have always been present to become more evident.

However, some industry observers suspect that the apparent increase is due to changes in the way inside wiring systems are interconnected. These changes may have created new surge coupling mechanisms. A particular area of interest is the possibility that surges on the AC mains are somehow being coupled onto communication cables.

One of the first applications to bring attention to surge failures on inside cables was the use of Optical Network Terminals (ONTs). Many telecom carriers have deployed systems which use a fiber optic cable to bring voice, data, and video service to a home or business. Somewhere on or near the building envelope the fiber cable terminates in the ONT. From there, metallic cable ports on the ONT connect to cables routed entirely within the building. Typical port types include Ethernet for data service, POTS (Plain Old Telephone Service) ports for traditional analog telephones, and coax cable for television service.

In an ONT, the POTS circuits are power feeding circuits known as SLICs (Subscriber Line Interface Circuits). These allow a conventional telephone to be connected to the ONT.

While this paper will use ONTs as a representative equipment type, the surge problem is not limited to ONTs. Manufacturers of VOIP telephone systems that support both Ethernet and POTS have reported similar problems.

As noted above, it is unclear whether the apparent increase in surge failures is simply due to more inside lines being deployed, or perhaps due to some other factor. For example, an annual failure rate of 1% might not attract much attention from a manufacturer with only 1,000 systems deployed in the field. Having ten systems per year sustain lightning damage might not appear excessive.

The situation changes if the manufacturer has one million systems deployed in the field. Now a 1% annual failure rate corresponds to 10,000 systems failing per year, so the lightning failures may attract more attention.

In the case of ONTs, there are several carriers that have more than one million systems in the field. And, since an ONT failure results in a service call to replace the failed unit, ONT failures are expensive for the carrier.

For most carriers, a failure rate of 1% is unacceptable. In fact, some carriers consider 0.1% to be unacceptable. So, it is possible that the lightning failures now receiving attention are simply due to more systems falling victim to the same coupling mechanisms that have always been present. Other observers think that the actual failure rates have increased recently due to new, unknown surge coupling mechanisms. In the following sections we will examine both possibilities.

II. CONVENTIONAL THEORY

Reference [1] describes the three commonly accepted coupling mechanisms by which lightning surges appear on communication cables:

- 1) Electromagnetic far-field coupling between the cable and the lightning discharge channel
- 2) Electromagnetic coupling between the cable and a down-conductor carrying lightning currents
- 3) Ground potential rise (GPR) forcing current through a cable that has different ground references at each end

In principle, inside cables are susceptible to all three of the above mechanisms, but the conditions for inducing large surges on inside wiring are limited. Mechanism 1 (far-field coupling), remains a threat for inside cables because most building structures provide comparatively little shielding from electromagnetic radiation. Wood structures provide almost no shielding at all, and many types of steel frame structures provide only limited shielding. So, a 300 meter cable strung inside a building has almost the same exposure to Mechanism 1 as it would have if it were strung outside the building.

For Mechanism 1 the key limitation for inside wiring is simply the length of the cable. Various studies of lightning induction on outside cables [2,3] have found that a cable of 5000 meters

will typically experience maximum surge voltages of approximately 5 kV in response to Mechanism 1. This implies that the maximum surge on a 300 meter cable would be proportionately smaller, corresponding to only 300 volts.

Mechanism 2 (down-conductor coupling) remains a distinct threat for inside cables, but only under limited conditions. This mechanism requires that lightning directly strike the building or the building's lightning protection system, and it also requires that the inside cable be routed for some distance in close proximity to a down-conductor that carries the lightning current. The down conductor can be either an explicit part of the building's lightning protection system, or it can be part of the building's steel frame. Mechanism 2 can indeed occur, but the required conditions are rare enough that it does not seem to explain the surge failures being observed in the field.

Mechanism 3 (GPR) requires that lightning current enter the ground near the building that contains the inside cables. The required proximity varies with a variety of factors such as strike current and soil conductivity [4,5]. For typical conditions, the required proximity for a lightning strike to generate a large GPR under a building is that the lightning current enter the ground less than 100 meters from the building. Furthermore, Mechanism 3 also requires that an affected cable within the building have its two ends connected to different ground references that are physically separated.

In principle, the electrical power distribution network in a building should have only a single ground reference, established by a ground rod located near the service entrance for the AC mains supply, as required by the National Electric Code [6]. If the building has only one ground reference, the inside cables can not be affected by GPR. In practice, some equipment installations have more than one ground reference, which creates the conditions that would allow a nearby lightning strike to induce surges via GPR.

To summarize, all three of the conventional mechanisms are indeed threats for cables routed entirely within a building, but the combined threat does not seem compelling. Mechanism 1 is expected to generate maximum surges of only a few hundred volts, while Mechanism 2 and Mechanism 3 require very specific conditions that limit the statistical likelihood that these mechanisms will generate damaging surges.

III. UNUSUAL CHARACTERISTICS OF OBSERVED FAILURES

Examination of damaged ONT ports [8,9] has revealed two rather surprising findings:

- 1) Ethernet ports, which typically contain a transformer-based isolation barrier that can withstand surges of at least 2 kV, often show clear evidence of catastrophic over-voltage failure of the isolation barrier.

- 2) POTS ports, which are typically not isolated and are conductively tied to ground at the ONT, often show clear evidence of over-current damage from lightning. Damage has been observed on POTS ports that were designed to withstand 100 amps for a short circuit current waveform of 2/10 microseconds.

So, on inside cables, there is evidence of voltage surges that exceed 2 kV, and evidence of current surges that exceed 100 amps peak for a 2/10 microsecond waveform. Since the cabling configuration of Ethernet differs from the cabling configuration for POTS, it can not be assumed that the same type of surge is affecting both port types. In other words, it can not be assumed that both port types are exposed to lightning surges with open-circuit voltages exceeding 2 kV and short-circuit currents exceeding 100 amps.

For example, since Ethernet ports contain an isolation barrier that generally prevents surge current from flowing to ground, very little current will flow unless the isolation barrier breaks down. Once the barrier breaks down, only a small amount of current is required to damage the Ethernet transceiver chip. So, in theory, a surge waveform with 3 kV open circuit voltage and only 5 amps short circuit current could damage a typical Ethernet port.

The reverse situation applies for a POTS port. These ports are typically ground referenced and are designed to source and sink current. Over-current protectors typically used in ONTs will survive lightning surge currents of 100 amps for a 2/10 microsecond waveform, while holding the voltage to less than 100 volts. So, in theory, a surge waveform with an open circuit voltage of only 300 volts and a short circuit current of 200 amps could damage a typical POTS port.

It is useful to note that vendors who have increased the surge tolerance of their Ethernet and POTS ports have seen significant reductions in field failure rates. Increasing the Ethernet isolation barrier to withstand 6 kV common mode surges appears to be very helpful. Similarly, increasing the POTS port surge tolerance to 500 amps for a 2/10 current waveform has been shown to be very helpful. It is not presently known whether these tolerance levels are actually required for controlling field failures, but they appear to be sufficient.

In summary, all that can be stated with certainty is that Ethernet ports are seeing open circuit surge voltages somewhere between 2 kV and 6 kV, and POTS ports are seeing short circuit surge currents somewhere between 100 amps and 500 amps (assuming a 2/10 microsecond current waveform). The precise distribution of surges within these ranges is not presently known.

Both of these ranges exceed what would normally be expected for all but very rare occurrences created by the conventional mechanisms described in the previous section.

IV. POSSIBLE MECHANISMS FOR OBSERVED FAILURES

Given the high open circuit voltages and short circuit currents, combined with an apparently high frequency of occurrence, some observers have suggested that there may be other coupling mechanisms at work. Such mechanisms could be operating in addition to the three conventional mechanisms described above.

One nearby source of sufficient voltage and current is the AC mains supply. Lightning surges appearing at a typical AC mains wall outlet can be quite large, with open circuit voltages of 6 kV and short circuit currents of 3 kA [7]. Furthermore, the AC mains system provides a path for lightning surges to be conductively transported to the interior of a building. There may be some non-obvious mechanisms that allow surges on the AC mains to couple onto inside communication cables.

Surges on the AC mains are considered a possible source because they have the requisite surge energy and they are present in close proximity to inside communications cabling. In view of this, various theories have been proposed to explain how surges on the AC mains could be conductively coupled to inside wiring for Ethernet and POTS:

- 1) Insulation breakdown through equipment that has both an AC mains power supply and Ethernet or POTS ports
- 2) Capacitive coupling through equipment that has both an AC mains power supply and Ethernet ports
- 3) Unintended interactions with customer-installed surge protectors that have both AC mains ports and Ethernet or POTS ports

The first theory is easy to understand, at least as a working theory. Most types of customer equipment connected to Ethernet and POTS ports also have their own AC mains ports. Examples would include computers and routers connected to Ethernet ports, and cordless phone base stations connected to POTS ports. For this theory, the main question to address is the likelihood of experiencing insulation breakdown from the AC mains port to the Ethernet or POTS ports.

The second theory (capacitive coupling) does not require insulation breakdown in the AC power supply, but this theory only applies to Ethernet failures. Almost all AC power supplies have a small but finite capacitance between the AC mains and the isolated output of the power supply. Surges with fast rise times on the AC mains can couple some amount of energy through this capacitance. Since Ethernet ports typically contain their own isolation barrier, the Ethernet isolation barrier is placed in series with the finite capacitance within the AC power supply. This creates a voltage divider where some fraction of the surge voltage on the AC mains appears directly across the Ethernet isolation barrier.

This theory can not be used to explain POTS failures. POTS ports are ground referenced and typically have overvoltage protection from the cable to ground, so it is generally not possible to develop high surge voltages on these ports. To damage a POTS port, it is necessary to force an excessive current through the port. The small amount of capacitance across the isolation barrier in an AC power supply is not enough to couple sufficient current to damage a typical POTS port.

The third theory (interactions with customer-installed surge protectors) is the most complex one to analyze, but this theory presents some interesting possibilities. The following sections will discuss each of the three theories in greater detail.

Theory 1: Insulation Breakdown

Fig. 1 shows a representative configuration of an ONT with an Ethernet port connected to a router, and a POTS port connected to a cordless phone base station. The power supplies for the router and the phone base station are wall mount supplies with a two-blade AC mains plug, so these two devices have no explicit connection to earth ground. However, the ONT power supply and its internal circuitry are typically grounded. A sufficiently large surge on the AC mains inputs

of the router or phone could cause a catastrophic breakdown of the isolation barriers that lie between those AC mains inputs and the earth ground at the ONT.

Referring to the Ethernet connection shown in Fig. 1, note that the surge path through the Ethernet cable would have to overcome three isolation barriers in series (Barrier 1, Barrier 2, and Barrier 3). Surge-to-failure testing on a random sampling of consumer equipment suggests that Barrier 1 typically has a surge-withstand of at least 9 kV, while Barriers 2 and 3 typically have a surge-withstand of at least 2 kV. So, it would appear that catastrophic breakdown of all three barriers in series would require a surge voltage exceeding $(9\text{ kV} + 2\text{ kV} + 2\text{ kV}) = 13\text{ kV}$. Such surges can appear on AC mains ports, but they are statistically rare.

Referring to the POTS connection in Fig. 1, it can be seen that there is only one isolation barrier (Barrier 4) standing between the AC mains port and the ground reference in the ONT.

Given that Barrier 4 typically has a surge withstand of at least 9 kV, any surges above 9 kV present the risk of catastrophic breakdown through the POTS port on the ONT to earth ground. This level is within the range of what might occur on an AC mains port, but it would be statistically very infrequent.

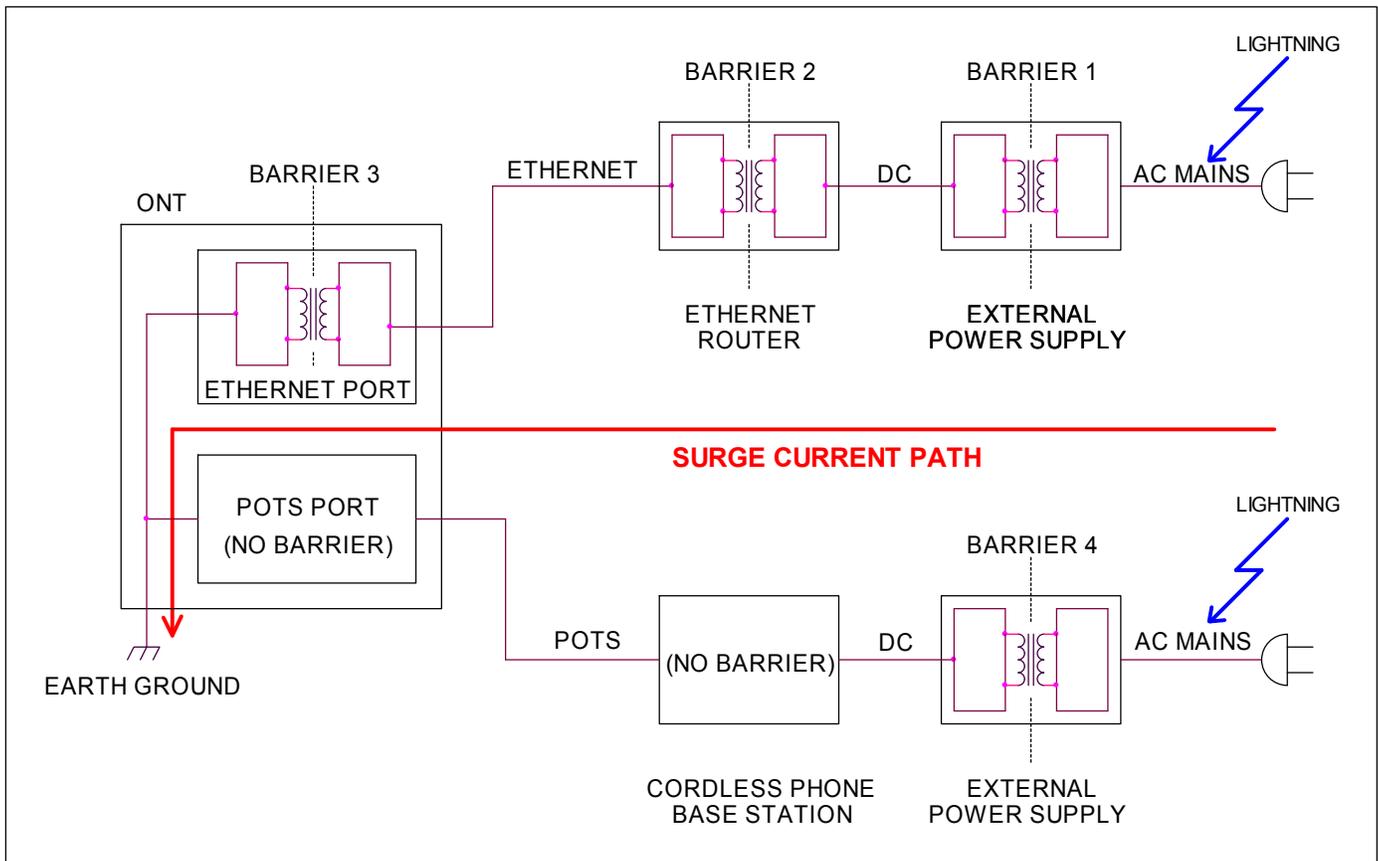


Fig. 1. Ethernet router and cordless phone base station connected to ONT

The above analysis is based on the assumption that AC mains power supply Barriers 1 and 4 have breakdown levels that “typically exceed 9 kV,” as determined via tests on a random sampling of consumer equipment. This finding is supported by the fact that AC mains power supply barriers are subject to compliance with safety regulations such as UL 60950-1 [10] that rigorously specify the isolation barrier.

Construction requirements placed on the AC mains isolation barrier include creepage distance, clearance distance, and distance through solid insulation. Some of the requirements are lower for a 120 VRMS mains supply than for a 240 VRMS supply, but most power supplies now sold in the USA are rated for both input voltages.

For a supply that complies with [10] and is rated for a 120 to 240 VRMS input, the isolation barrier’s creepage distance and clearance distance will be in the range of 4 mm, distance through solid insulation will exceed 0.4 mm, and the production hipot test will be 3000 VRMS (4242 volts peak). In practice, power supplies that are designed to meet the construction requirements in [10] typically have actual surge breakdown thresholds above 9 kV.

Interestingly, some generic replacement power supplies purchased on the internet showed breakdown levels as low as 3 kV. Internal inspection revealed that the isolation barriers in these supplies were not compliant with [10]. These non-compliant supplies had no safety markings from independent labs, although they did have the CE marking for manufacturer’s self-declaration in Europe.

At present there is no evidence of non-compliant power supplies being used by name brand manufacturers of routers and cordless phones. So, for the purposes of the present analysis, a minimum breakdown threshold of 9 kV has been assigned to wall mount power supplies. However, it is worth noting that some power supplies available on the market have lower breakdown thresholds.

For the Ethernet isolation barriers that were found to have a surge tolerance that “typically exceeds 2 kV,” this finding seems reasonable given that the Ethernet standard IEEE 802.3 [11] requires an isolation barrier rated at 1500 VRMS, which corresponds to 2121 volts peak. Note that [11] is simply an industry standard rather than a regulatory standard, so there is no formal enforcement of this requirement. However, virtually all commercially available Ethernet transformers are rated by their manufacturers to have 1500 VRMS isolation.

Most Ethernet interfaces also contain a capacitor that bridges the isolation barrier. This capacitor is the subject of the following section and will be discussed in greater detail there.

In summary, catastrophic failure of the isolation barriers in Fig. 1 seems to be an unlikely candidate for explaining the unusual surge failures under discussion here. This is particularly true

for Ethernet ports, since catastrophic breakdown would likely require surges of greater than 13 kV. Even for POTS ports, the required surge level would likely exceed 9 kV.

Theory 2: Capacitive Coupling Through the AC Power Supply

Fig. 2 shows a representative configuration of an ONT with an Ethernet port connected to a router. In this case the capacitance across each of the three successive isolation barriers is explicitly represented by capacitors C1, C2, and C3.

It is important to understand that these are not just parasitic capacitances from parameters such as inter-winding capacitance in the transformers. Rather, each capacitor is a physical, high voltage capacitor intentionally placed across the isolation barrier by the circuit designer.

Capacitor C1 appears in almost all switching power supplies and has a typical value of 2200 pF. Its purpose is to control conducted emissions on the AC mains. The maximum value of C1 is limited by safety requirements regarding touch current on the isolated output of the power supply [10]. In some cases C1 can be larger than 2200 pF.

Note that capacitor C1 is not required in a linear power supply that combines a 60 Hz step-down transformer with a linear regulator, since there is no switching noise to mitigate. In a linear supply, the capacitance represented by C1 is just the parasitic inter-winding capacitance of the 60 Hz transformer. Typical values for this parasitic capacitance are in the range of 100 pF.

Up until a few years ago, most small Ethernet routers used a wall-mount linear supply for power. Due to increasing regulatory requirements for energy efficiency, wall-mount linear supplies have been mostly phased out in favor of wall-mount switching supplies. So, the presence of an explicit capacitor C1 in the power supply for small Ethernet routers is a recent change. As will be seen, the value of C1 has an effect on the surge voltages that are coupled from the AC mains to the Ethernet ports of the router and the ONT.

Capacitors C2 and C3 are used in most Ethernet ports to reduce common mode emissions and to reduce susceptibility to conducted RF. A typical value is 1000 pF.

Using typical values of 2200 pF for C1 and 1000 pF for C2 and C3, we find that for a surge between the router’s AC mains input and the ONT ground, approximately 18% of the surge voltage appears across C1, 41% across C2, and 41% across C3. Note that reducing the capacitance of C2 and C3 will increase the percentage of the surge voltage that appears across them. Increasing the capacitance of C1 will also increase the voltage across C2 and C3.

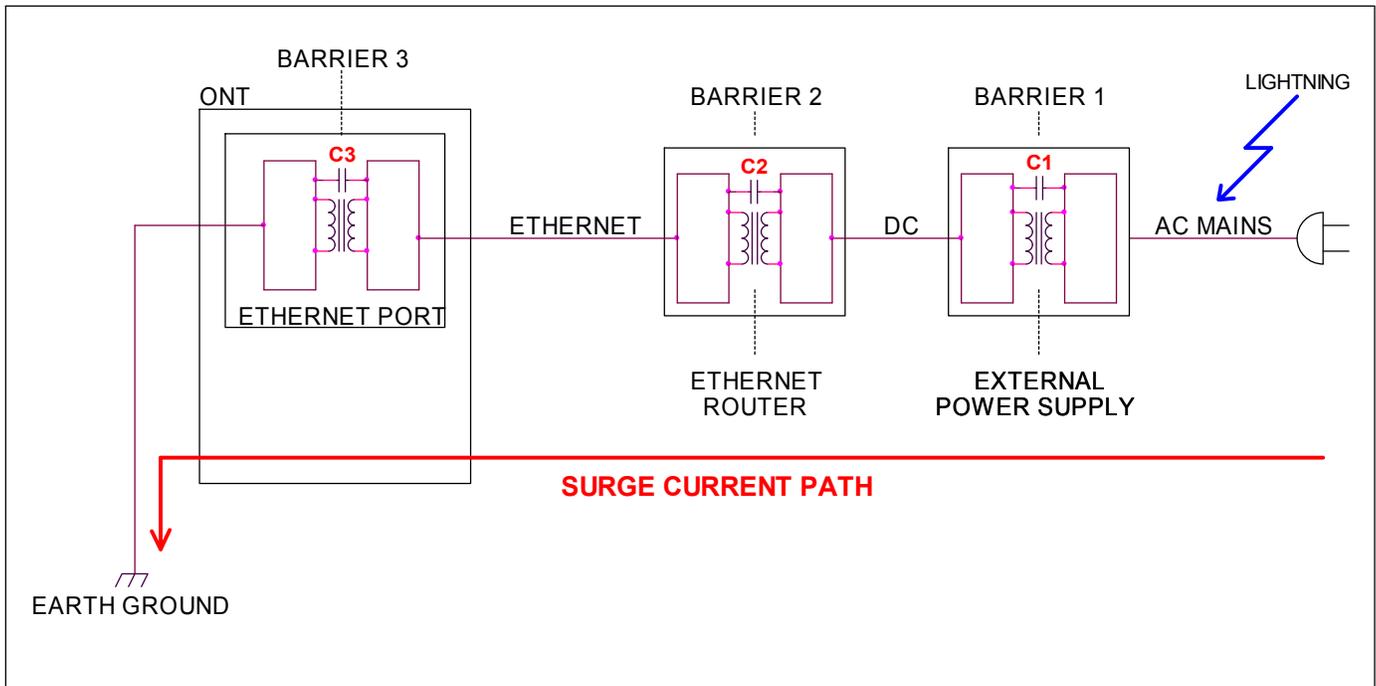


Fig. 2. Capacitive coupling path through Ethernet router

Typically, capacitor C1 is a robust high voltage capacitor because it bridges a safety isolation barrier and is subject to careful scrutiny during the safety evaluation of the AC power supply. It will be a so-called “Y1” capacitor because of its classification in [12] as a component that is permitted to bridge a safety isolation barrier. Y1 capacitors for 240 VRMS mains are rated to withstand multiple 8 kV surges. Their actual failure threshold is usually much higher.

On the other hand, capacitors C2 and C3 are usually not safety-rated capacitors because the isolation barrier in an Ethernet port is not generally considered to be a safety isolation barrier. For most applications, indoor Ethernet cables are classified as SELV circuits per [10]. This puts them in the same class as the internal circuits to which they connect in most computers and routers, so no form of safety isolation is required by [10].

However, in a properly designed Ethernet port that complies with IEEE 802.3, these capacitors and the associated Ethernet transformer will be rated to survive a 1500 VRMS AC or 2250 VDC hipot test because this level of isolation is called out in IEEE 802.3. The isolation requirement in IEEE 802.3 is generally believed to have originated as a functional requirement intended to provide robust immunity to common mode interference, but the actual origins of this requirement are unclear.

For the present analysis, the important thing to understand is that C2 and C3 are not typically treated as safety-rated capacitors and are not reviewed by safety agencies. Furthermore, the isolation requirement in IEEE 802.3 is only a functional requirement that appears in a voluntary industry standard. So, there are no regulatory agencies looking at these capacitors, and there is little incentive for design engineers to pay much attention to these capacitors. Most manufacturers never even perform the IEEE 802.3 hipot test to confirm that their design meets the 802.3 isolation requirement.

As a result, C2 and C3 are usually selected by individual designers who may not be thinking about hipot tests and surge tolerance. In most product designs, the capacitors used for C2 and C3 are small surface mount components with voltage ratings that allow them to just barely pass the isolation tests in IEEE 802.3.

This makes C2 and C3 likely candidates for isolation breakdown if higher than expected surge levels are encountered. Surge energy can be capacitively coupled through C1, which typically suffers no damage, due to its robust construction as a safety-rated capacitor. C2 and C3 are more vulnerable because they are less robust and because they frequently have lower capacitance values than C1. These lower capacitance values cause C1 and C2 to experience a greater proportion of the total surge voltage.

Examination of Ethernet ports that suffered isolation breakdown in the field often shows a damaged capacitor and no damage to the associated transformer.

Theory 3: Unintended Interactions With Customer-Installed Surge Protectors

There are several ways that surge protectors could unintentionally create surges on Ethernet and POTS ports. Due to the range of possible customer installation configurations, the variety of possible mechanisms is quite large, and not all of them can be discussed here. The following discussion will focus on just two possible mechanisms:

- 1) Open ground
- 2) Ground wire inductance

Fig. 3 is a photo of several representative “combination surge protectors.” Each of these devices combines surge protection circuits for four port types: AC mains, Ethernet, POTS, and coax. Common variations of the combination surge protector omit one or more of the four port types, but the individual protection schemes used on each of the remaining port types will be similar to the circuits described here.

Fig. 4 shows a very simplified schematic of the internal circuitry in a combination surge protector. It is important to understand that while several surge protection components are used on multi-conductor ports such as Ethernet and POTS, the diagram in Fig.4 represents these as a single device on each port type. This simplification has been made so that the discussion can focus on common mode surges.



Fig. 3. Combination surge protectors

The surge protection components commonly used for protection on an AC mains outlet are MOVs (metal oxide varistors) with threshold voltages of approximately 400 volts. Similarly, MOVs are the most common type used on POTS ports, although the threshold voltages are typically in the range of 300 volts. The most common components used for Ethernet protection are TVS diodes with thresholds of approximately 70 volts, typically in combination with a set of steering diodes that allow a single TVS diode to protect all four pairs in the Ethernet cable. For coax protection, most surge protectors use GDTs (gas discharge tubes) with threshold voltages of approximately 100 volts.

The circuit of the combination surge protector in Fig. 4 creates opportunities for a surge on the AC mains to be conductively passed to each of the other port types that the surge protector is designed to protect. Any surge protector that combines a protected AC mains port with any other port type will present this risk.

The simplest coupling risk occurs if for some reason the ground connection used by the surge protector is left open. Since the surge protector of Fig. 4 intentionally ties all of the ports together through comparatively low voltage protection components, the only thing that prevents surges on one port from appearing on all other ports is a reliable connection to earth ground.

This is easy to visualize by imagining the connection to ground at point A in Fig. 4 to be open. With Point A open, surges that appear on the AC mains port are not taken to ground through point A. The next best path to ground is through one or more of the protected ports connected to the ONT.

The key point here is that lightning surges will always seek the lowest impedance path to ground. The proper functioning of surge protectors like the one in Fig. 4 is entirely dependent on having a low impedance path to ground via their ground connection at the AC wall outlet. If for any reason this ground becomes unreliable, surge currents will seek the next-best path to ground. That path could be through a piece of equipment that the surge protector was intended to protect. The ironic aspect of this is that having a combination surge protector with an unreliable ground can be worse than having no protector at all.

While it is easy to see how a missing ground on a combination surge protector would readily couple surges from the AC mains directly onto every other port, it seems unlikely that this mechanism could explain the number of surge failures that have been experienced in the field. After all, most surge protectors are correctly plugged into an AC wall outlet that accepts a plug with a ground pin, and most wall outlets have this ground reliably connected back to the ground rod at the service entrance for the AC mains. Exceptions certainly do occur, but are probably not widespread.

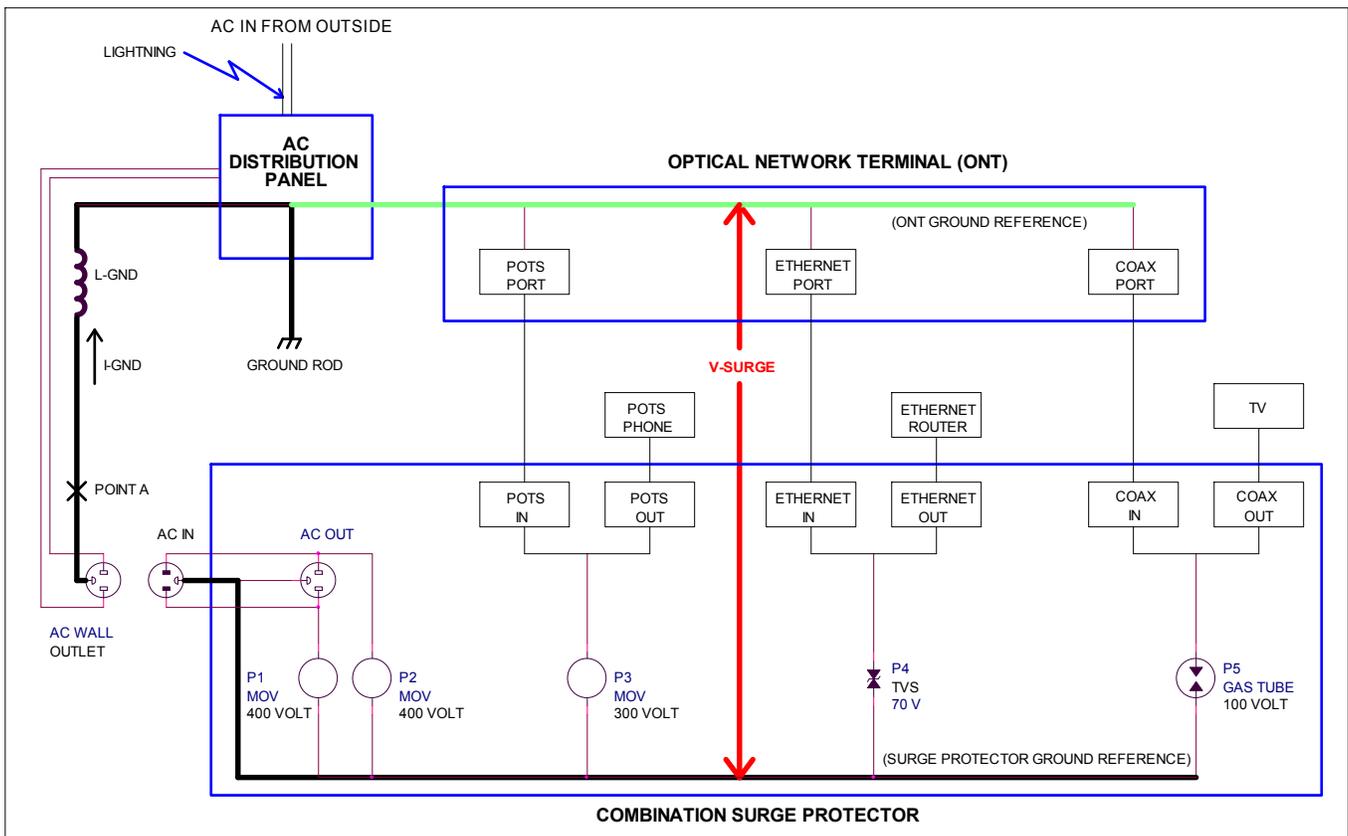


Fig. 4. Household wiring diagram with combination surge protector installed.

However, the type of damage that can occur with a missing ground connection on the surge protector can also occur even if the ground is correctly wired back to the ground rod at the service entrance. The reason this can occur has to do with the inductance of the ground wire.

A single wire has a small but finite amount of inductance, typically in the range of 2 microhenries per meter. So, a 50 meter ground wire that connects a surge protector to the ground rod will have approximately 100 microhenries of inductance.

In the case of the ground wire associated with an AC power outlet, a length of 50 meters would not be unusual. The ground wires associated with AC mains outlets in a building are typically wired in a star configuration that originates from the electrical panel at the AC mains service entrance. The central ground node in the electrical panel is, in turn, connected to a ground rod by a wire that is usually quite short. So, while the central ground node in the electrical panel can be considered to be a low impedance ground, the same can not be said about the ground presented at a given electrical outlet.

At AC power frequencies of 50/60 Hz, a 100 microhenry inductance creates a negligible impedance. However, for a fast rising surge waveform, this same inductance can create a very high impedance. To understand how this occurs, recall

that the voltage V across an inductor L is represented by the following expression, where di/dt represents the rate of change of the current in the inductor:

$$V = L(di/dt)$$

A representative lightning surge on the AC mains might have a short-circuit current waveform of 500 amps peak with a rise time of 8 microseconds [7]. Applying these values to a 100 microhenry inductor, the calculated voltage comes out to 6.25 kV.

This calculation oversimplifies the situation for a surge waveform that has an exponential rise time, but the basic principle remains valid. Large surge currents with fast rise times can generate voltage drops of several thousand volts on a long ground wire.

Returning to Fig. 4, consider what happens when a lightning surge appears on the AC mains outlet. Protection components P1 and/or P2 turn on at nominally 400 volts, and the surge current attempts to flow through the AC outlet's ground wire back to the electrical panel. If a 6 kV voltage drop develops across the length of the ground wire (represented by L-GND in Fig. 4), the entire ground reference node within the surge protector rises to an instantaneous potential of 6 kV above earth ground.

This has the effect of lifting the surge protector end of every connected cable (AC mains, Ethernet, POTS, and coax) to an instantaneous value of 6 kV above earth ground. At this point, surge currents that would normally be expected to exit through the ground connection may find other, more attractive paths to ground through the connected cables.

The key point here is that a high current, fast rise time surge on the AC mains can interact with the inductance of the ground wire to create a high voltage common mode surge on every cable that is connected to the surge protector. In some sense, the surge protector takes a surge on the AC mains and “broadcasts” it onto every cable that is connected to the surge protector. This happens despite the fact the surge protector has been installed correctly and the ground wire of the AC mains outlet is connected properly.

An interesting aspect of this surge mechanism is that the equipment co-located with the surge protector is usually not damaged by the surge, since the surge protector and all the co-located equipment have approximately the same voltage potential rise with respect to earth ground. Damage occurs in the equipment connected to the far end of the cable over which the surge current managed to flow. So, if the surge current found a path to ground through an Ethernet port or POTS port on an ONT, the only thing damaged as a result is the port on the ONT. To the customer, it appears that the ONT had some sort of isolated problem that was unrelated to any other part of the customer’s installation.

Reference [13] contains an excellent description of the risks created by improper use of surge protectors. In principle, these risks can be mitigated by careful analysis of the interconnected equipment and the grounding within the building. Based on the findings of this analysis, surge protectors are placed at strategic points in the building.

Unfortunately, most users are not technically qualified to perform the required analysis. Most users will simply purchase a surge protector and install it near the equipment they wish to protect. They may not realize that doing so has the effect of directing surge currents to other equipment located elsewhere in the building.

V. SUMMARY

In recent years, many suppliers of telecom equipment have experienced higher than expected rates of lightning surge damage on Ethernet and POTS ports that connect only to inside wiring. The resulting physical damage indicates that surge voltages exceeding 2 kV are occurring on Ethernet ports, and surge currents exceeding 100 amps (for an assumed 2/10 microsecond current waveform) are occurring on POTS ports. These levels are not easily explained by conventional

assumptions about how lightning surges couple onto cables routed entirely within a building.

While at least one of the known conventional mechanisms (GPR) is capable of creating such large surges, the required conditions are comparatively rare. It appears that some other mechanisms may be at work.

Various theories for alternate mechanisms have been put forward by industry experts. Three of these theories have been discussed in detail. All three of these theories are based on the notion that surges on the AC mains are somehow being coupled onto inside Ethernet and POTS cables.

The analysis suggests that the first of these theories seems improbable, and the second theory, while quite plausible, can only be used to explain failures involving isolation breakdown in an Ethernet port. This theory does not explain POTS failures.

A third theory centers on unintended side effects of customer installed surge protectors. Such devices have become more common in recent years. The third theory can produce damage that matches the observed failures on both Ethernet and POTS ports.

A useful next step for testing these theories would be to gather data on actual field failures to try and match their characteristics to one of the candidate theories.

For example, Theory 1 will result in damage to the equipment connected to the associated port. Theory 2, which applies only to Ethernet ports, results in no damage to the connected equipment, and more importantly, involves relatively low surge currents. The damage resulting from Theory 2 would show very little physical evidence such as melted circuit board traces or charred materials. However, close inspection may reveal arc traces in certain areas within the port, or internal damage to integrated circuits. Theory 3 can couple very high energy surges onto either POTS or Ethernet ports, without causing damage to the connected equipment. However, Theory 3 only applies to cases where the customer has installed a multi-port surge protector.

Unfortunately, manufacturers of equipment with Ethernet and POTS ports have little control over the characteristics of the power and grounding environment into which their equipment will be installed. This means that even if field evaluations confirm that the mechanisms of any of these theories are causing the observed failures, there is little that manufacturers can do to prevent the surges from occurring.

While the theoretical mechanisms presented here should be subjected to further study, manufacturers who wish to immediately reduce their field failure rates can take certain steps without necessarily understanding the underlying causes.

It appears that increasing Ethernet common mode surge tolerance to 6 kV is sufficient to eliminate most failures of the Ethernet isolation barrier. Increasing POTS surge current tolerance to 500 amps for a 2x10 microsecond current waveform appears to be sufficient to eliminate most surge failures on POTS ports.

REFERENCES

- [1] J. Randolph, "Introduction to lightning and AC power fault surge protection for telecom signaling cables," 2012 IEEE Symposium on Product Compliance Engineering.
- [2] Bell Communications Research, *Lightning, Radio Frequency, and 60-Hz Disturbances at the Bell Operating Company Network Interface*, TR-EOP-000001, Issue 2, June 1987.
- [3] *The Protection of Telecommunications Lines and Equipment Against Lightning Discharges*, Chapter 10, ITU 1995
- [4] A. Martin, *Lightning damage to equipment without a metallic connection to an external communications service*, In Compliance Magazine, September 2011
- [5] A. Martin, *Lightning induced GPR*, In Compliance Magazine, June 2012.
- [6] NFPA 70, "National Electric Code," 2014 Edition, National Fire Protection Association.
- [7] IEEE C.62.41.2, "Recommended Practice on Characterization of Surges in Low-Voltage (1000V and Less) AC Power Circuits," IEEE Power Engineering Society, 2002.
- [8] M. J. Maytum, "Lightning damage of home network ports," 2011 ATIS PEG conference.
- [9] J. B. Wiese, "Optical network terminals (ONTs): lightning damage and standards – what's the latest information?," 2013 ATIS PEG conference.
- [10] UL 60950-1, Second Edition/CAN/CSA C22.2 No. 60950-1-07, "Information Technology Equipment – Safety – Part 1: General Requirements," Underwriters Laboratories Inc. and Canadian Standards Association.
- [11] IEEE 802.3-2002, "Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications."
- [12] IEC 60384-14, "Fixed Capacitors for Electromagnetic Interference Suppression and Connection to the Supply Mains," June 2013.
- [13] "How to Protect Your House and its Contents From Lightning," IEEE Guide for Surge Protection of Equipment Connected to AC Power and Communication Circuits, IEEE Press, 2005.