PROVIDING A SAFE HOME FOR YOUR PEPLINK ROUTER

Business
Continuity
from
an Engineering
Perspective

- 01

THE MITIGATION OF THREATS

NATURAL PHENOMENON,
THREATS,
CHALLENGES,

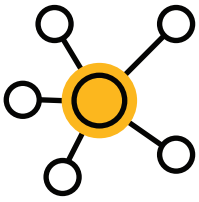
THE MITIGATION OF THREATS

Businesses throughout the world face a myriad of threats, the components of which change over time and location. In one area the enterprise may be challenged by natural phenomenon – lightning, floods or extreme heat. In another location the threats may be civil unrest, vandalism or organized crime. Indeed, governments often face the exact same threats as the privately and publicly-held businesses within their jurisdiction. Therefore, the strategies suggested herein apply to all environments where critical data communications equipment is installed.

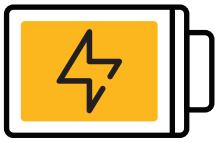
This whitepaper focuses on the mitigation of threats to a critical element of operations – data communications – internet, client-server communications between branch and headquarters, between government offices, telephony, etc. In today's world communications are vital to the heart of the enterprise. We'll look at some of the main threats to such communications and how these challenges can be mitigated.

While it may be a relatively simple (OK, well, sometimes very technically challenging) task to buy hardware, install it and "make it work," let's look beyond this obvious step and think about the big picture and try to visualize the router, switch and other infrastructure as part of a vital and resilient system which must be protected. For our example let's install a Peplink Balance 20X and discuss how we can best protect both it and the other vital equipment and resources it touches.

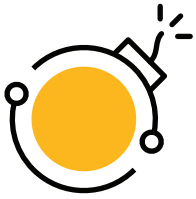
In the author's experience the principal challenges lay in several main areas:



01
Providing for multiple, redundant paths for critical data



02
Ensuring the reliability and quality of power



03
Reducing threats to circuits that enter the premises

While it may be challenging to do a "perfect" implementation at the outset of the installation, every step taken to harden the infrastructure and provide for redundancy will be rewarded with increased reliability and survivability.

Fortunately, there are good, well-proven solutions to each of the aforesaid concerns. Let's take them one-by one ...

- 04

PEPLINK'S BALANCE 20X

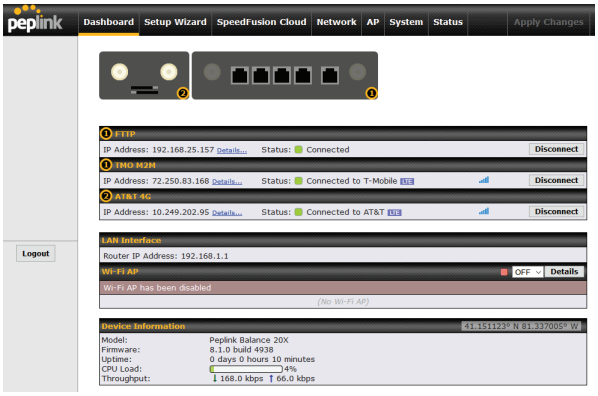
PROVIDING FOR MULTIPLE, REDUNDANT PATHS FOR CRITICAL DATA

Executives and IT professionals alike recognize the importance of communications – internally, with customers, suppliers, regulatory agencies ... the list goes on and on. Indeed, the stories which involve sustained failures of such systems often result in loss of revenue, loss of customer confidence and occasionally, business failures. In today's world these communications are mainly digital, the analog world being an artifact of an earlier era. So, the fundamental task is to provide for reliable, redundant, and effective data communications.

The decision as to which router to employ is a fundamental one. For our example here, we have an internet provider that can provision relatively reliable service. However in the interest of business continuity it would be unwise to rely on any terrestrial service for 100% of one's requirement. A logical choice would be to add a cellular/4G WAN which may be used simultaneously with the 1GB WAN or as a back-up only.
For our example we'll choose Peplink's Balance 20X. The 20X is a near-gigabit-class router with built-in 4G. The latter provides for redundancy in a "single box."

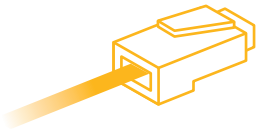
Indeed, an additional cellular module can be added – all the way up to a CAT-18 modem if needed. When 5G is available a suitable module can be added to provide that capability if desired.
Although the 20X has a single ethernet port for WAN, a second wired WAN can be added via the router's versatile USB port. So, the 20X can handle four WANs: Ethernet via it's RJ-45 port, ethernet or cellular via its USB port, Cat4 cellular via built-in modem, and an optional cellular module.

The 20X is a PrimeCare device which includes SpeedFusion "out of the box" – Peplink's innovative Gartner "4th Quadrant" SD-WAN technology. SpeedFusion Cloud, can also be added quite inexpensively.
In our case we'll connect the ISP's service to the Ethernet port. For the 2nd WAN we'll use a CAT-12 module. The built-in cellular module will be used with a low data-rate M2M SIM. The latter is a very inexpensive service which will be used as the primary WAN for certain on-premise M2M devices and as a last resort to "call for help" if the primary WANs were to fail.

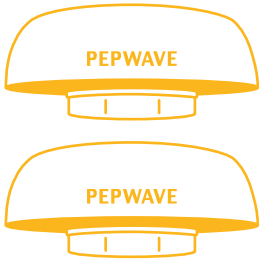


So, to get started we'll need the following connections:

Power (using the provided power supply)



Ethernet from the ISP's MODEM



Two antennas (one for each cellular module)

The final installation will be no more reliable than the most vulnerable of these connections. To make the system reliable there are a number of other considerations that should be addressed. Indeed, we'll see that buying and installing a Peplink router is the easy part. So, let's take some time and do this right!

ENSURING THE RELIABILITY AND QUALITY OF POWER

PART 1
UTILITY POWER

Fortunately, the solutions to the “power problem” are generally rather well-known and relatively easy to solve. First, one should access the need for a replacement for utility power. While the most common arrangement is to install a back-up generator, and that’s what we’ll use here, other solutions such as a solar system may work in certain environments. The selection of a generator is not trivial matter and among the questions that must be answered are:

WHAT TYPE OF FUEL TO BE USED?

The generator could be powered by natural gas, propane or diesel fuel. Gasoline? Perhaps, but this is generally not the best solution.

HOW MUCH FUEL SHOULD BE PROVIDED FOR?

The fuel reserves are an important consideration and should be planned to outlast the expected duration of an emergency. This is easy to do if powered by a reliable source of natural gas but is a bit more challenging when using propane or diesel. Indeed, liquid fuels present additional challenges such as stability of the fuel and a safe method of storage.

TYPE OF GENERATOR?

This is a “big” decision! The main criteria that drives this decision is the expectation as to how long it will be used at a given time as well as required service life. Among the issues are these:

LIQUID OR AIR COOLED?

Generally, liquid-cooled equipment lasts longer but requires a bit more maintenance

SPEED?

Generators which run faster, say 3600RPM, are less expensive and usually have shorter service lives than do those that run slower, perhaps 1800RPM.

WHAT SHOULD BE POWERED BY THE GENERATOR?

Ideally, the entire facility of course! If that’s not possible then a decision must be made as to “what’s important.” Regardless, an automatic transfer panel should be incorporated as part of the solution.

For our purposes here we’ll omit considering the use of a portable generator. While such equipment often has a role to play in keeping an operation running, it’s best to focus on “hands-off” solutions that “just work.” (We’ll be coming back to that theme again!)

PART 2
POWER FOR CRITICAL EQUIPMENT

Temporary replacement for utility power was discussed in the preceding paragraphs. But no generator can pick up the load from a failed electric utility immediately. In actuality the sequence of activities looks something like this, although the time associated with each step or process can vary considerably.

1. Utility power fails
2. Failure of primary power is sensed by the transfer panel (milliseconds)
3. A timer is started and after a pre-set time instructions are issued to start the generator (varies; perhaps 15-30 seconds)
4. Generator warms up a bit and voltage and frequency are stabilized (15 seconds to one minute)
5. The transfer panel switches the load from the dead utility power supply to the generator.

So, what happens between the time the first and last events occur? Bad things! Computers crash and as the data communications infrastructure loses power, IP telephones go dark and all communications with the outside world is lost.
So, this points up the requirement for the survivable enterprise to have two forms of back-up power. The first must carry the load for hours, days or even longer, and is most likely to be a generator, as discussed above. The second is an uninterruptible power supply. One is generally never a substitute for the other.

Essentially, one UPS device is required for each piece of equipment that cannot be permitted to fail. This would typically include communications and data communications systems, routers, switches and the racks that contain them. Equipment throughout the building such as servers, wireless access points and IP telephone must have their own UPSs if not powered by POE, power over Ethernet. (This, by the way, is a strong argument for the use of POE.)

AS IS WITH THE CASE WITH GENERATORS, UNINTERRUPTIBLE POWER SUPPLIES ARE AVAILABLE IN MANY VARIETIES. HERE ARE THE MOST IMPORTANT VARIABLES:

TYPE OF OUTPUT?

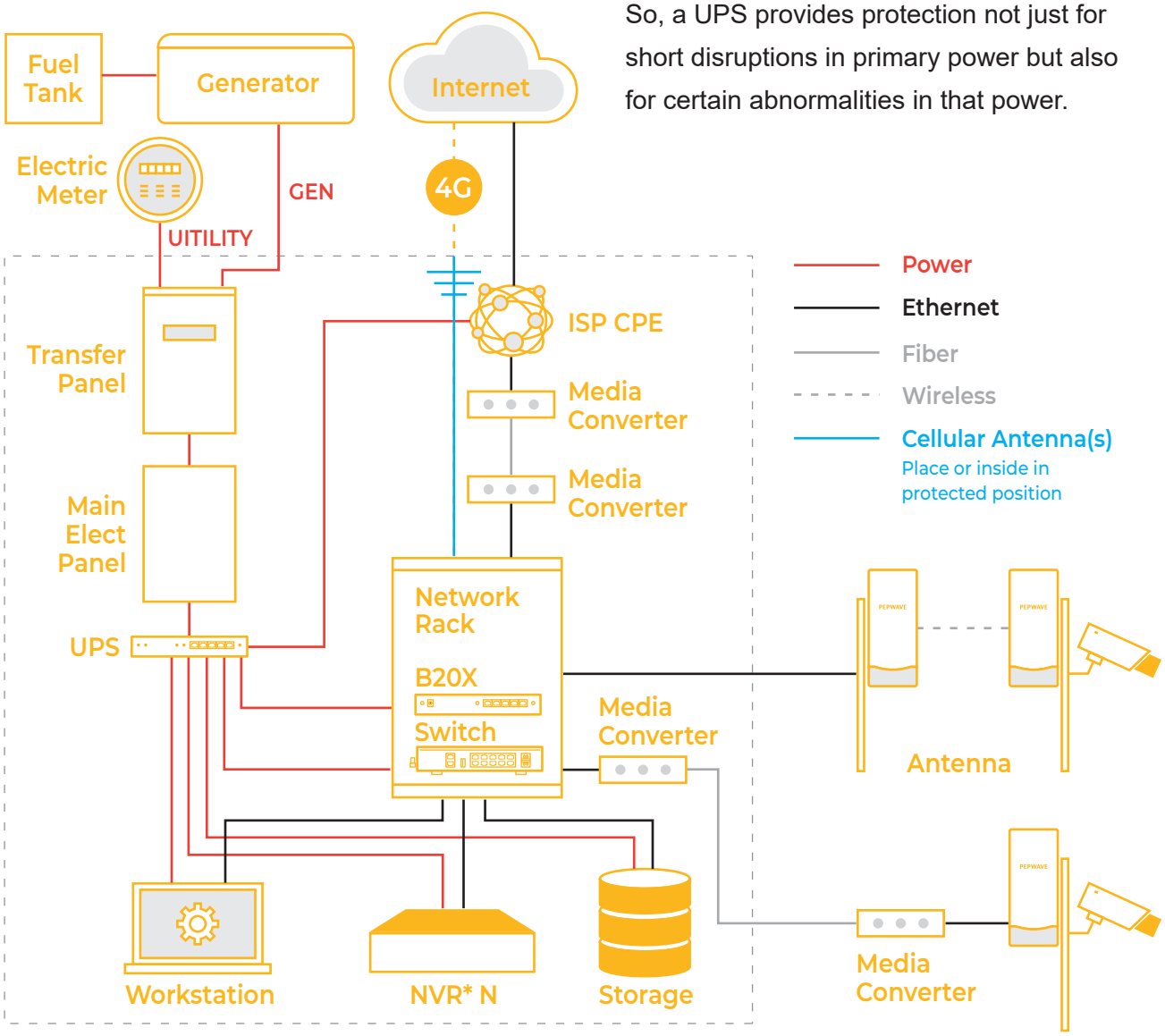
The decision as to whether sine wave output is required or modified sinusoidal wave is acceptable is based on the requirements of the equipment to be powered. The former is more expensive, as may be expected. (Generally, Peplink equipment runs fine on most good quality UPSs – even if the output is not a perfect sine wave.)

RUN TIME?

The purpose for a UPS in this environment is only to power the critical equipment between the time utility power is removed and the load is transferred to the generator – not for use for an extended period. So, “theoretically” the UPS battery(ies) need only last for a very few minutes. However, the tendency to increase the load on UPSs over time is well known and over time the UPS batteries become less efficient. So, it’s best to provide a bit of margin vis-a-vis run time.

So, the most obvious and well-recognized rationale for employing an uninterruptible power supply is to provide power for essential equipment until the main back-up system, typically a generator, comes on-line. However, there's an additional rationale which is less commonly recognized. While the loss of utility power may be the most dramatic event and the one that catches one's attention the quickest, it's not the only threat. The quality of utility power is highly uneven around the world. A well-designed UPS can protect against voltage sags, high voltage, and certain transients. Indeed, many of the well-known manufacturers exhibit confidence in the quality of their products that they provide insurance for the equipment behind the UPS if the former is damaged.

So, a UPS provides protection not just for short disruptions in primary power but also for certain abnormalities in that power.



SUPPRESSING THREATS TO CIRCUITS THAT ENTER THE PREMISES

Here our objective is to avoid or mitigate damage to critical infrastructure where the point of origin is outside the building which houses the enterprise. There are three main areas where action is typically recommended:

01
Protection of Utility Power at the Electric Panel or Meter

02
Grounding and Bonding

03
Isolation of Critical Circuits and Components from Terrestrial and Environmental Threats

PROTECTION OF UTILITY POWER AT THE ELECTRIC PANEL OR METER

The value of using uninterruptible power supplies to protect certain high value equipment was discussed in the preceding section. And, indeed, a UPS does that well. However, the first step, and one that is often omitted when engineering the power distribution system is to add a power protection device at the electrical service panel. Alternatively, in some jurisdictions, such a device can be located outside the premises in the electric meter base. Regardless, the purpose of such a device is to shunt high voltage which may appear on the power line to ground. The addition of this equipment greatly increases the probability that the various components within the building that are connected to AC power will survive events such as lightning which results in direct contact with the outside conductors, induced current caused by electromagnetic pulse or a phase-to-phase short.

GROUNDING AND BONDING

"Grounding" provides a means to transmit high levels of electrical energy to ground. "Bonding" is the technique used to ensure all components of interest are at the same electrical potential. While the former term is often used (incorrectly) to mean the latter, grounding and bonding are really different concepts – but both are absolutely required.

The electrical engineer or contractor must design a low impedance ground system to which all critical equipment can be bonded. One may note that the design requirements of the ground system may significantly exceed that which electric codes may prescribe for electric service if delicate electronic equipment is to be effectively protected.

While many volumes have been written about the theory and practice of grounding and bonding, the essence of this requirement is that all equipment is "tied" to a single-point ground near the electrical service entrance. The conductors should be as short as possible, with maximum surface area and without any more bends or turns than necessary. It's critical that a low impedance path to ground is provided.

ISOLATION OF CRITICAL CIRCUITS AND COMPONENTS FROM TERRESTRIAL AND ENVIRONMENTAL THREATS

When considering our options to protect the enterprise's power supply our options are limited to providing for a back-up, adding surge suppression and grounding/bonding solutions. However, when we consider other penetrations of the building shell we have some additional tools which may be brought into play. So, how do we protect WAN data circuits, LAN data circuits, and transmission lines between cellular antenna(s) and routers? There are essentially three methods:

01
Light gap

02
Radio gap

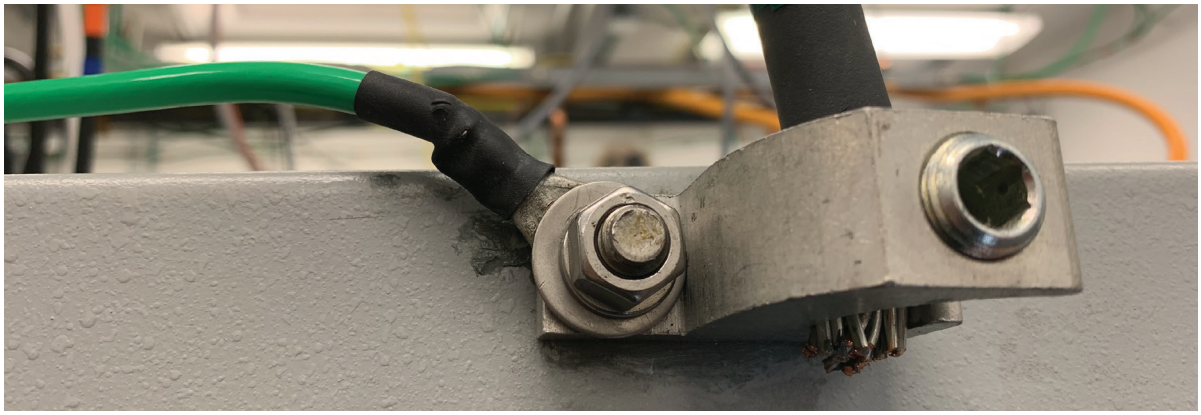
03
Making the component invisible to the threat

Essentially, our objective here is either to "break" the path of electrical current while ensuring the performance of the circuit is unimpaired or to install the component in such a manner as to protect it from threats. Let's look at both approaches.

Imagine a situation where one of the primary WANs is "cable internet" and the MODEM is connected to one of the WAN ports of the building's router. Without action on our part a voltage "spike" or induced current on the coax cable

connected to the MODEM and may travel on to the router's WAN port via the Ethernet cable. The results could be devastating. In such a case the MODEM and router may not be the only victims. One must also consider downstream switches and other networked components. A relatively easy and inexpensive solution: Insert a media converter at each end of a short length of fiber optic cable. Now there is no electrical path between the component at risk (the MODEM) and the valuable assets (the router and other networked equipment.) The photo shows one end of the "light gap" – at the MODEM. A second media converter would be located at the router. The same principle was used to protect the path from IP CCTV camera located on a radio tower adjacent to the building. It's not difficult to imagine the damage to network infrastructure that could result from a lightning strike to a 30m high steel tower.

Another means to break the electric path between devices near the perimeter of the building is "radio." One may use a microwave path or a device as simple (and effective) as a Peplink Device Connector. In the latter case the device connector acts as a wi-fi bridge between the device that is at risk and the on-premise wi-fi network. Easy!



The third method to protect our network is to position the vital components in such a manner so as to protect them from threats. And, this is the strategy we'll use as we consider how we'll install the antenna(s) for the Balance 20X router. In the simplest case we may find that the antennas furnished with the router may be quite sufficient. If so, that makes things quite easy. Often, however, more complex antennas must be employed. Where should we place these antennas? We often see recommendations such as "high and in the clear." Indeed, in considering performance (alone) that is a good strategy. But performance often increases risk.

Recommendation: Try to situate the antenna (or antennas) as low as possible ***consistent with adequate performance***. Use existing structures to shield the antenna from lightning if possible. In the example case some easy experiments were undertaken before final positioning. Fortunately, in this suburban environment cellular signals from multiple carriers were strong. While the antennas furnished with the Balance 20X were sufficient, it was found that adding antennas, one for each module, brought the signal levels and quality up to a point where excellent throughput was obtained. The "back-up plan" was to place them in the building's attic but this was not required.

Conventional wisdom strongly suggests using a lightning suppression device on all antenna transmission lines. While this is certainly a good practice experience has shown the results are not always as promised – even when high quality devices are employed. Indeed, no such device will protect against a direct strike. Shielding the antenna from such a phenomenon, or "making it invisible" to the forces of nature will yield far greater – and more certain – benefits.

WRAPPING IT UP

Acquiring, installing and properly configuring a SD-WAN router is an important step to take in ensuring the continuity of the enterprise. Indeed, many stop there and do little else. However, this paper has outlined various strategies to help optimize the chances of survival of the data communications system: ensuring the continuity of good quality primary power and protection against lightning on utility power lines, WAN circuits and the router's cellular antenna. Recommendation: Take every reasonable step to ensure survivability and reliability – even if resources permit this only to be done over time.

Rick Patterson
PSS Telecom Management
peplink@commtower.com
November, 2020