**This Issue:**

Troubleshoot Performance Issues with These 3 Network Cabling Tips

When it Rains, it Pours – Keep Your Cloud-Based Data Safe

Be the Life of the Party: Server Hosting

Use a Firewall Before You Get Burned

Mobile Technology Gains the Lead in Computing Race

USB Software is Bad to the Bone, Literally

---

**Troubleshoot Performance Issues with These 3 Network Cabling Tips**

When you experience an error or a performance issue with your company's computer system, you will troubleshoot the problem in hopes of resolving it quickly. Before you open the case of your hardware and start messing with components, check your cables. Even a small cabling issue can cause big problems with your entire network.

Setting up your network and installing cables properly is a surprisingly-delicate procedure that requires a plan called "cable mapping." It's vital that your cables are properly handled. If a cable is defective due to a lack of planning, then it can hinder productivity and even cause downtime. The next time you encounter a networking issue, try out these three cabling tips.

**Clean Your Connectors**

Remember the old video game cartridges from Nintendo? If you inserted it into the game incorrectly, it would not work. The same goes for network cables. A dirty or damaged connector can cause problems. Clean your connectors with a soft brush or a cotton swab.

**When it Rains, it Pours – Keep Your Cloud-Based Data Safe**

Do you see those black clouds culminating on the horizon? They represent the possibility that hackers will gain access to your cloud storage. Though it is protected a number of ways, it will not stop an experienced hacker. To them, your defenses are as transparent as those thin, wispy, cirrus clouds that are so welcome on a boiling hot summer day.

When it comes to cloud storage security, there are a number of things that you should keep in mind:

**Use Obscure Words or Phrases for Your Password**

Cloud storage starts with a password, but sometimes, hackers can find ways around them. This doesn't mean that passwords are not safe, but it does mean that the possibility is there, and cannot be ignored. Hackers commonly use brute force tactics, where they attempt to crack the code by randomly inputting passwords. Though this process could take a long time, some hackers are likely more tenacious than you think, and won't give up so easily if they truly want your data. Make sure that your password utilizes lower-case and upper-case letters, as well as numbers and symbols.

Another way to protect your data is to use less-common words for your password, or make up your own, rather than use a common word. Doing so puts you at risk of a dictionary attack, which involves a hacker inputting common passwords. Think about the amount of people who use the word "password" to keep their data safe. Their data isn't so safe if the hacker assumes that they chose an obvious word for their password. Instead, opt for strange or obscure phrases. For example, "D3epSeaRh1n0F1shing#$9" will have hackers guessing for ages.

---

**Be the Life of the Party: Server Hosting**

When it comes to hosting a party, it can be exhausting – it's a matter of space, cost, and responsibility, among other things. If you're too busy trying to organize everything, nobody will get to see the best side of you. Wouldn't it be so much easier to just hire someone to take care of the details? You would actually be able to enjoy your party!

Ground Swell's managed server hosting allows just that. We'll take care of all the little details so you can concentrate on what is really important – your business, and your clients. With managed server hosting from Ground Swell, not only will you never need to worry about your server again, but you'll discover that it is ideal for your business needs.

**Remain Flexible**

When arranging a party, you'll

(Continued on page 4)
Troubleshoot Performance Issues with These 3 Network Cabling Tips

console and it didn't work, what did you do? You would remove it and blow on it like it was some kind of ocarina (of time). Why did you do this? Gamers implemented this best practice because they thought blowing on the game would remove the dust from the cartridge's connectors and provide a working signal. Often times, this troubleshooting practice would work like a charm and you'd be saving the Mushroom Kingdom again in no time!

In the same way, a dirty cable connector end face can be the cause of performance issues across your system. In fact, this is the surprising top cause of network issues. Resolving an issue can be as easy as blowing on your cable ends. However, for maximum cable cleaning, Processor magazine recommends digging deeper:

Use a simple handheld microscope to inspect the end face. If you detect contamination, there are several good fiber optic cleaning products that can quickly remove the contamination and return the connector to a clean/usable state.

Check for Microbends
When cables are improperly handled and installed, they bunch up, become twisted, and get pinched. You may be thinking, "No big deal," but the reality of cable management is that even a small bend, what's known as a cable micro-bend, can disrupt the flow of data and cause performance issues. The best way to avoid such twists and bends is to plan out your network's cable layout so that all of your wires are as straight as possible.

Measure the Power Levels
Your networking cables are able to move data with the assistance of electricity. If the power levels are abnormal, then the flow of data will be hindered. Therefore, being aware of your cable’s power levels will be of great assistance in helping you identify which cables are underperforming and should be replaced. To check the power levels of your cables, you will need a simple power meter. Use the meter to measure the power levels at your different connection points, and make a note of the weaker connections. Try replacing the weaker cables with new ones and see if there’s a performance boost.

A good IT technician, such as those here at Ground Swell, are familiar with other tools that can judge the quality of your console and it didn't work, what did you do? You would remove it and blow on it like it was some kind of ocarina (of time). Why did you do this? Gamers implemented this best practice because they thought blowing on the game would remove the dust from the cartridge’s connectors and provide a working signal. Often times, this troubleshooting practice would work like a charm and you’d be saving the Mushroom Kingdom again in no time!

In the same way, a dirty cable connector end face can be the cause of performance issues across your system. In fact, this is the surprising top cause of network issues. Resolving an issue can be as easy as blowing on your cable ends. However, for maximum cable cleaning, Processor magazine recommends digging deeper:

Use a simple handheld microscope to inspect the end face. If you detect contamination, there are several good fiber optic cleaning products that can quickly remove the contamination and return the connector to a clean/usable state.

Check for Microbends
When cables are improperly handled and installed, they bunch up, become twisted, and get pinched. You may be thinking, "No big deal," but the reality of cable management is that even a small bend, what's known as a cable micro-bend, can disrupt the flow of data and cause performance issues. The best way to avoid such twists and bends is to plan out your network's cable layout so that all of your wires are as straight as possible.

Measure the Power Levels
Your networking cables are able to move data with the assistance of electricity. If the power levels are abnormal, then the flow of data will be hindered. Therefore, being aware of your cable’s power levels will be of great assistance in helping you identify which cables are underperforming and should be replaced. To check the power levels of your cables, you will need a simple power meter. Use the meter to measure the power levels at your different connection points, and make a note of the weaker connections. Try replacing the weaker cables with new ones and see if there’s a performance boost.

A good IT technician, such as those here at Ground Swell, are familiar with other tools that can judge the quality of your

When it Rains, it Pours – Keep Your Cloud-Based Data Safe

storage. While many storage clouds will encrypt the data while it is traveling, you still want to be wary and avoid web applications that do not have "https" in front of the URL. The "s" informs the user that the text’s data is a secure, encrypted protocol, and therefore, safe.

Hackers are Lazy
They might work pretty hard to get to your data, but in reality, hackers will likely utilize the easiest means possible to retrieve said data. This generally involves attacking the cloud storage itself rather than your personal data. This can mean that the hacker may not even care about your data and leave it alone, but do you want to take that risk? It’s best to use a cloud storage well known for having superior security.

Lock Your Password Away and Swallow the Key
Figuratively, not literally. Keep your password to yourself, and never tell it to anyone. Some hackers will try to get you to fork over your valuable information themselves by claiming to be a service provider, but don’t be fooled. If you aren’t sure if you want to trust an unknown cloud source with your precious data, give Ground Swell a call at (609) 487-9100. We can provide your business with a secure cloud storage solution to fit your company’s needs, and we’ll do our utmost to ensure that you don’t muddle through the oncoming storm alone.

Call us today to save money with your IT expenses. You will be surprised by how easy it is!

http://bit.ly/1sArcTH

Share this Article!
Use a Firewall Before You Get Burned

Too many people think that their systems are safe from the corruption of hackers and viruses. They’re wrong. In order to keep your business safe from all of the common threats found on the Internet, you should think about installing some protective software.

One of the most useful types of protection is a firewall. The term originally referred to a wall built to confine a fire within a building, but in this case, a firewall is a type of software that keeps your company safe from the dangers found on the Internet. Believe us when we say that a little protection can go a long way.

What Does a Firewall Do?

When data flows in and out of a network, the firewall is the software that analyzes it. It acts like a bouncer, in a sense. It keeps anything that could damage your computer out of it. Basically, it’s a barrier between your network and data that is deemed unsafe and insecure. These threats will most likely be found while surfing the Internet.

Like any barrier, there are many different types of firewalls that vary in strength. These barriers can investigate network traffic, validate connection and data packets, check for legitimate application data, and perform cavity searches on all messages going to and from your network. They are updated regularly to battle against the latest threats, but they’re certainly not immortal.

What Doesn’t a Firewall Do?

The firewall is definitely a good bet to stop some dangerous activity, but it doesn’t solve all of your Internet problems. It’s important to understand what you’re vulnerable to, even with a firewall, so you know what to avoid and how to deal with threats. Viruses, spyware, adware, and phishing scams are examples of malicious software that bypass the protection offered by firewalls. In addition, firewalls also fail to protect you from infected email attachments or block spam, which can be counterproductive and annoying.

USB Software is Bad to the Bone, Literally

USB devices have long been a staple of the technology world, but are notoriously vulnerable to exploitation from hackers and malware. As malware grows more and more sophisticated, you can no longer trust simple antivirus scans to protect your business.

Unfortunately, it has less to do with what the USB carries than what it is made out of. Researchers Karston Nohl and Jakob Lell plan on presenting their findings which dictate that USB software is fundamentally broken; in other words, it’s the software itself that is the problem, not what the devices themselves contain. Nohl and Lell created a type of malware called BadUSB, which when installed on a USB drive and can potentially compromise a computer, alter files installed with the drive without being detected, and mess with the user’s Internet browsing.

Bad to the Bone

BadUSB lives up to its name due to how difficult it is to locate, essentially post-exploitation. BadUSB lies within the firmware that controls the functions of USB devices, not in the flash memory storage of them. This lets the attack code remain undetected even after the device’s storage has been deleted or scanned by antivirus software.

What’s even worse is that this isn’t a problem that can be fixed. The total compromise that BadUSB displays is impossible to counter completely (unless USB drives are banned altogether – something that is both inconvenient and frankly, not possible for most PC users). It’s not as simple as patching software, as the vulnerability lies in rewriting the code within the device.

What are my Options?

One of the best security options we can provide your company with is called a Unified Threat Manager (UTM) from Ground Swell. The UTM is a combination of a strong firewall and other powerful security tools designed to provide protection for your entire network. Most firewalls that initially come with a PC offer so little protection that it might as well be unprotected, but the UTM is a whole different monster.

UTMs vary in shape and size depending on your company’s needs, network size, and network traffic. Ground Swell can outfit your system with the perfect UTM for your business. We can even provide your company with a free network security audit to patch up the holes in your current firewall. Ground Swell can be your own personal firefighter, putting a stop to the catastrophic digital fires that threaten your company.

Too many people think that their systems are safe from the corruption of hackers and viruses. They’re wrong. In order to keep your business safe from all of the common threats found on the Internet, you should think about installing some protective software.
Be the Life of the Party: Server Hosting

(Continued from page 1)

never know how many people will show up. It will start as a group of close friends coming over to play Cranium, but your best friend brought his girlfriend, and his girlfriend brought her besties with her, and your cousin brought his best friend’s uncle’s daughter with him, and so on. Before you know it, your house has no food, your brain hurts, and you have a mess to clean up.

Bandwidth is the same way; you might think you can control it, but there are too many variables to take into account. Things like your local Internet Service Provider (ISP) and consumer variables can make your bandwidth fluctuate greatly. Instead of worrying about something you can’t control, let Ground Swell deal with it for you. We’ll assess your Internet connection before we host your data to see if it has what it takes to support your company’s data needs. You might need to upgrade your networking equipment, such as your wireless router, or we can help you find a new ISP that will be better suited to your needs. There’s no reason to hire a new staff member just to solve your bandwidth problems.

No Need to Buy New Equipment
Having the latest technology means regularly upgrading the equipment and hardware, and if you’re the one hosting your server, these can leave your wallet hanging up high and dry. Rather than upgrading all the time, let the server host take care of this. We at Ground Swell can use our resources to update your

We’ll take care of all the little details so you can concentrate on what is really important — your business, and your clients. With managed server hosting you never need to worry about your server again...

server, which is far more cost efficient for you. New gear is extraordinarily expensive in the end, and your budget will crumble because of it. By using Ground Swell’s services, you are labeling these upgrading expenses as an operating expense rather than a capital expense, making your budget much more flexible in the end.

We’ll Monitor Your Server for You
When we host your data, we will be the ones to resolve any problems that come up. You don’t need to worry yourself with them. You can depend on Ground Swell always being there for you. We’ll monitor the servers, fix hardware failures, or problems in the network. Nothing will happen to your data on our watch!

Your Data is Safe with Us
Ground Swell also looks after your data and ensures that it is properly backed up and securely protected. We use enterprise-level firewalls, remote monitoring software, and our team of professional IT technicians to keep your data from malicious hackers and software. We’ll do whatever we need to do to keep hackers away from your data.

The benefits of Ground Swell hosting your server far outweigh the costs. At Ground Swell, we’ll be the host so you can enjoy your party. Call us today at (609) 487-9100 and we’ll take care of your data needs.

Ground Swell will provide your organization with flexible IT support that helps keep you competitive and without breaking the bank.

Justin Tinel, President

We'll take care of all the little details so you can concentrate on what is really important -- your business, and your clients. With managed server hosting you never need to worry about your server again...

About Ground Swell

We are a technology consulting firm specializing in technology implementation and management for businesses. We’re known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses at an affordable price.

Ground Swell will provide your organization with flexible IT support that helps keep you competitive and without breaking the bank.

Justin Tinel, President

Ground Swell

6712 Washington Ave
Suite 305
EHT, NJ 08234
609-487-9100

Visit us online at:
newsletter.gswell.net
facebook.gswell.net
linkedin.gswell.net
twitter.gswell.net
blog.gswell.net

No Need to Buy New Equipment

About Ground Swell

We are a technology consulting firm specializing in technology implementation and management for businesses. We’re known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses at an affordable price.

Ground Swell will provide your organization with flexible IT support that helps keep you competitive and without breaking the bank.

Justin Tinel, President

Ground Swell

6712 Washington Ave
Suite 305
EHT, NJ 08234
609-487-9100

Visit us online at:
newsletter.gswell.net
facebook.gswell.net
linkedin.gswell.net
twitter.gswell.net
blog.gswell.net