EnableIP
WAN UPTIME EXPERTS

Network Down? Here Are The Most Common Reasons Why

The 5 biggest problems resulting in network outages for business (and how to prevent them)

Depending on what drives profits for your particular business, you may have seen the chaos that can ensue as soon as users lose access to the WAN and the applications it enables. A room full of productive employees turns into mindless zombies staring at their screens or phones, at a total loss of what to do next. This scenario is if you’re lucky. The alternative is a room full of screaming angry employees demanding answers and a solution.

Either way, it’s not a pretty sight to say the least…

One of the most important steps to take when planning for a highly available WAN is to identify the most common causes of network downtime so that you can plan for as many of them as possible. In the world of networks, there are many variables that can’t be controlled, so it’s very important to control what you can.

By planning for as many of the most common causes of network downtime as possible listed below, you can increase your productivity and decrease company downtime.

1. ISP Outages

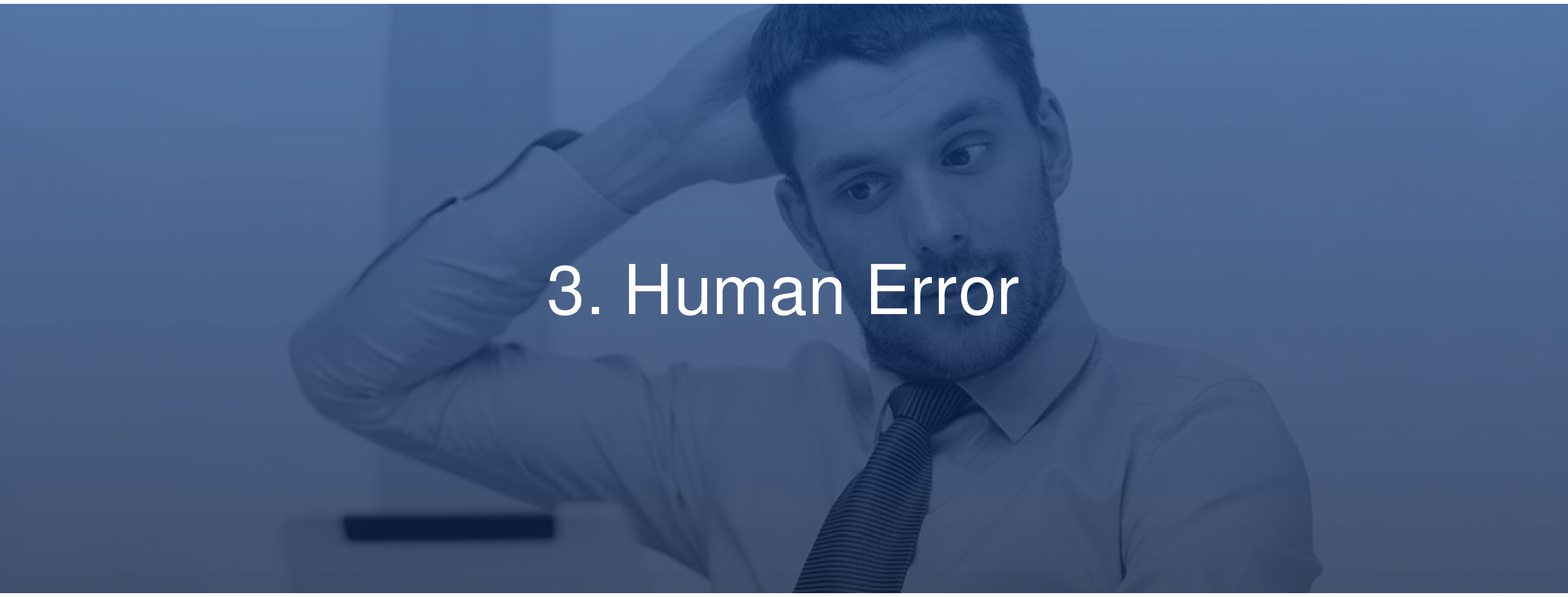
One of the most common ways a WAN can go down is for an ISP to have an outage of some kind. Not all outages are created equal and the downtime created by these can range from minutes to days. The causes of these outages can range from fiber cuts to core outages, and the average time to repair will change based on the original cause of the outage. In the end, they all fall under the category of an ISP outage and the cause of the outage doesn't make it any less painful or disruptive to your business.

The theory behind addressing ISP outages is simple, but the follow-through can be tricky. The end goal is to create redundancy and diversity. All sites should have multiple WAN connections that are as diverse from each other as logistically possible. This helps make sure that road construction or some other mishap is less likely to take down both connections at once. By making sure both connections are on diverse carriers, the possibility of a core outage taking your entire network down becomes a non-issue. Be redundant, be diverse and you'll stay up and running!

2. Technology/Device Failure

Whether you pay less than $100 for your network hardware or thousands of dollars per month, you still run the risk of having your hardware fail you. The idea of redundancy is just as important when it comes to hardware as it is when talking about WAN connections. It's important to identify where the single points of failure are in your network and predict which hardware components are most likely to fail or the hardest to replace. A single piece of hardware crashing can take all of your users down just as quickly as a fiber cut or power outage.

Preparing for these issues is easier to plan for and completely within your control. While you have no control over *when* a device will fail, you can have pre-configured spares ready so that downtime is minimized as much as possible. While it may be an added investment upfront to have extra hardware ready, it will pay off when something goes down (as it inevitably will) and you don’t have to wait for a new device to be purchased, shipped, configured and installed.



3. Human Error

Human error can range from a poor deployment of network components or hardware to a misuse of a perfectly functioning network. Whether the network is actually down or a user is accessing it incorrectly, the end result is an employee who is unproductive. Identifying the source of the human error can be tricky, especially since pride comes into play and the individual involved may not want to admit any fault in the problem.

Preventing human error is impossible, but minimizing it is a realistic goal. From a deployment standpoint, having a detailed plan with contingencies in place and testing all components before installing them can go a long way in making sure the network functions as planned. Testing after installation is equally important to make sure that everything works in the field the same way it did in the lab.

When it comes to user error, it gets a little more tricky. All employees have a varying level of technology knowledge, so some users will be more prone to incorrect network usage than others. The best you can do is to offer consistent and detailed training on all new applications and portals to employees so that they have the information they need on how to use the tools that keep your business profitable.

4. Natural Disasters

We’ve got good news and bad news. Let’s get the bad news out of the way:

There is nothing you can do to prevent natural disasters and you usually aren’t going to get much in the way of warning before one happens. Some things are truly out of our control and this falls into that category.

Okay, so what’s the good news?

Modern WAN infrastructure is resilient and it takes a true disaster to take most networks down. They certainly can happen (Hurricane Harvey, Hurricane Katrina, Snowmageddon, etc.), but most likely this isn’t an issue you will have to deal with very often.

The main advice we’d like to give here is to make sure that you have a *nimble network architecture* so that if only one of your sites goes down, the rest can still communicate with each other. It’s also worth noting that you will want any hosted applications or servers — whether you host them in data centers or are using a third party such as a SaaS provider — are redundant and geographically diverse. If your sites are depending on the information they get from a data center, you will want to make sure there’s a backup data center that’s far enough away from the primary network that the same natural disaster can’t take both of them down.

5. Cyber Attacks

While ISP failures, natural disasters, human error and technology failure are the primary reasons that networks tend to fail, hacking and cyber attacks on networks are increasingly becoming a serious threat in recent years.

According to Ponemon Institute's "2016 Cost of Data Center Outages" report:

> *Cybercrime represents the fastest growing cause of data center outages, rising from 2% of outages in 2010 to 18% in 2013, to 22%…*

The frequency and sophistication of cyber attacks are skyrocketing, and their effects on businesses continues to rise. Dyn, an Internet infrastructure company, experienced a wave of DDoS attacks in 2016, resulting in a massive outage that affected sites including Twitter, Etsy, Github, Vox, Spotify, Airbnb, Netflix and Reddit.

If you don't have the personnel on staff to secure your network, then investing in a partner that can accomplish this for you is a necessity so that you aren't putting your users and customers at risk — on top of risking unnecessary downtime.

Network Downtime Solutions

While there are countless things that can lead to network downtime, the most common causes addressed above can, for the most part, be planned for. By taking proactive steps and planning for the most common potential problems, you are setting up your users and your business for the best network experience possible.

If you have ongoing issues or don't have the expertise needed, then find a partner who can fill the void. The investment you make will come back tenfold in employee productivity due to decreased downtime.

Are you ready to get serious about network downtime? Plan to succeed with EnableIP.

About EnableIP

EnableIP is a telecom solutions provider founded by Wired Networks' founder Jeremy Kerth and head engineer Steve Roos after they realized there was a deep market need for helping mid-size businesses establish better uptime rates for their Wide Area Networks (WANs). Armed with the best-in-class carriers and partners, Jeremy and Steve set out with a bold plan: **Guarantee better uptime rates than the industry standard of only 99.5%.**

Their bold plan became a reality. EnableIP's solutions guarantee clients 99.99% (even 99.999%) network uptime. But we don't stop there. Many telecom providers promise high availability network solutions but fail to deliver because they're in the business of providing services, not solutions.

That's the EnableIP difference: We deliver highly available networks by providing a complete system (called "Cloud Assurance") that ensures 99.99% or above uptime.

We deliver this bold promise by:

- ✓ Owning the entire customer experience. From pricing, contracting, ordering and provisioning to installing, servicing and billing—we do it all! This means no stressful negotiations, confusing setups, or finger pointing if something goes wrong. We actually *deliver* on our promise.
- ✓ We manage the entire system, and monitor and manage issues as they occur so you can focus on your business—not your network.

The EnableIP solution is like no other. Contact us to get started and experience the difference of a system that truly delivers on its 99.99% network uptime promise.

EnableIP
WAN UPTIME EXPERTS