EnableIP
WAN UPTIME EXPERTS

Essential Networking Hardware for Mid-Market Businesses

A comprehensive small business network setup checklist

So your small business is growing and thriving into the mid-markets — congratulations!

With growth, though, comes a whole new set of challenges. As you expand, establishing good standard practices and setting the foundation to grow on could be what determines *how much* and *how fast* you're able to continue growing.

In a world where technology has gone from a neat business add-on to a necessity, it's important to make sure you are building a network that is **secure**, **reliable** and **keeps your users in touch** with their applications and profitable.

The very core of that foundation is your basic networking hardware.

Choosing the right version of each element discussed below is a complicated process unique to each business's needs. Identifying what you need from your networking hardware is essential, and if you don't have an IT professional on-staff to help you with this process you may want to consider bringing in a consultant.

Just because a router is "amazing" in a review doesn't mean it will be a good fit for your needs. We can help you identify the most important features for your users and find the solution that best fits those needs — starting with following hardware essentials.

Firewall

It may sound like something from *Game of Thrones* or *The Hobbit*, but a firewall is simply a device that controls data flow from the interior of your network to the exterior (and vice-versa).

Do you want to be the next company on the news because some hacker got into your network and stole all of your customer’s data? (We’re looking at you, Target.)

Then, we strongly suggest you select the right firewall and be cognizant of where your other networking hardware is in relation to it. Like a physical wall, in order for it to offer any protection a device needs to be *behind* the firewall. A wall can’t protect what’s standing in front of it.

Firewalls protect against many different types of attacks. It’s important to know what type of attacks your network is most likely to experience and make sure your firewall solution is equipped to deal with them. A firewall is also an important tool in allowing multiple sites to safely communicate with each other and pass data.

Some important features to explore in firewalls include:

- **DDOS prevention**. A denial-of-service cyber attack is when the hacker or attacker seeks to make a machine or network resource unavailable to its end users by temporarily or indefinitely disrupting services of a host connected to the Internet.
- **IDS/IPS**. Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyzes signatures too, but can also stop the packet from being delivered based on what kind of attacks it detects — helping prevent the attack.
- **VPN**. VPNs implement site-to-site encryption and anonymize your IP address so that hackers, governments, and even your ISP can only see that you connected to a VPN server — they won’t know what you’re looking at or what you’re doing on the internet.
- **Proxy server**. A proxy server changes your IP address and masks the origin of your network traffic by acting as an intermediary between your computer and the internet.

It’s worth noting that many times a firewall exists within a router. Many modern hardware solutions can act as a router, firewall, modem and switch — all within the same piece of hardware. Depending on the number of users you’re trying to support at each site, this can be a great solution for you. As the number of end-users grows, the less realistic this option becomes.

Router

If the firewall is the bouncer at a nightclub, then the router is the manager. Routers make sure things are operating as they’re supposed to and that everybody is doing their job so that customers are having the optimal experience.

The correct router for you will be determined by many factors, such as WAN architecture/technology, the number of users supported, the need to communicate with other sites or cloud services, your necessity for WAN optimization tools, and the amount of overall throughput it needs to support.

Note: The full list of factors to consider when choosing a router is really quite extensive, but these are some common factors to be explored. Consult your IT staff or hire a consultant to fully evaluate your options and understand your needs.

It’s also important to mention that your router selection — and firewall for that matter — should be able to support multiple WAN connections. The last thing you want is your company to be “single threaded” to its wide area network. Choose networking equipment that can immediately pivot from one WAN connection to another to keep your users working and productive.

Switch

Have you ever walked into a networking room (or “nerd-closet” as we affectionately call them) and seen a device with countless ethernet ports plugged into it? If so, you were most likely looking at a switch.

A network switch (also commonly referred to as a switching hub, bridging hub, and MAC bridge) is a computer networking device that uses packet switching to receive, process, and forward data to the destination device.

Switches not only offer an Ethernet handoff to devices through your locations, but can also be essential in prioritization of certain traffic. Different ports on switches can be configured for different types of traffic based on what type of device is on the other end of it.

Selecting a switch that allows you the control you need over each port and can support the throughput your network requires is vital. Here are three basic types of switches available (as defined by NeweggBusiness.com:

- An **unmanaged switch** is the likely choice for most small business networks. It works out of the box and offers only basic configuration features. Unmanaged switches require minimal technical aptitude to install and operate. In short, they just work.
- A **managed switch** gives you more control over how your network consumes an Internet connection. Usually IT controls a managed switch using the command line interface (CLI), but newer managed switches do have a graphical interface to use. Managed switches can be adjusted remotely, ideal for large-scale or satellite office deployments. A managed switch generally requires some technical training to take full advantage of their feature set.
- Several manufacturers market a **smart switch**, also called a Layer 2/3 switch. A smart switch is an in-between for unmanaged/managed switches. It’s ‘smarter’ than an unmanaged switch because it gives you control over Layer 2 of the open systems interconnection (OSI) model. However, if you need full-on Layer 3 controls for your small office network, opt for a managed switch.

Computers

You’re building an amazing network so that your users can leverage applications. But in order to do that, they’ll need a way to interface with these tools.

This is where some form of computing device comes in to play.

These days, computers can be anything from a desktop or laptop, to a phone or tablet. Let’s briefly explore some of the more common computing options below.

Desktops

Let’s kick this discussion off by going “old” school. Desktops have their advantages, even in today’s ever mobilizing landscape. For one, they’re less expensive for the same computing power than their mobile counterparts. They’re also easier to take apart and work on or upgrade. If the computer is being used by a static user with no need to be on the move, then it can be the perfect solution.

As users continue to utilize more and more applications at the same time, it’s also worth mentioning that most desktops can readily support multiple monitors, allowing for a less crowded visual workspace. Many laptops have to use their screen, usually much smaller, as the primary screen and can use only one other screen of your choosing. There are exceptions, but they tend to be higher-end laptops that will hit your wallet harder.

Laptops

Laptops are becoming the workhorse of today’s workforce. They’re mobile, powerful, and have a battery life that continues to grow with every iteration that comes out. Laptops offer companies the ability to provide the majority of their users with a single device they can use to be productive from practically anywhere.

Gone are the days of buying every employee a desktop *and* a laptop (Thank heavens!), as today’s laptops are more than powerful enough to operate as both. Users can either use a laptop at their desk, or leverage a docking station or similar technology to imitate the feeling of a more traditional workspace and take advantage of ergonomic keyboards and an external mouse.

Tablets

In recent years, tablets have been making the leap from a nifty device for distracting children to a viable business technology that even further mobilizes today's workforce. Even smaller and lighter than a laptop, tablets are the epitome of mobilization. No, we didn't forget that smart phones exist, but many users prefer a larger workspace for their applications, making a tablet a better overall business solution.

As tablets continue to grow more powerful and function on the same operating systems as most laptops, their adoption across a variety of industries is bound to increase as well. An early hindrance to their adoption was their unique operating systems forcing users to use mobile versions of their most important applications, which was less than ideal. Many modern tablets can run the same version of any given application as their laptop counterparts.

Thin Clients

Thin clients are relatively new and many business owners aren't very familiar with them yet. You can think of a thin client as a "dumb" terminal that, on its own, isn't much more than a monitor. These devices were created to enable cloud-based computing. If the cloud is doing your computing, then why invest in a tablet, laptop or desktop that has computing power of its own?

Thin clients have only enough intelligence to connect to the network and stream data from a computer existing in a server or data center off-site. Thin-clients are simple and cheaper than traditional computing solutions, with not much that can go wrong. They also serve as a cheap option for connecting users to off-site computing assets like VDIs and Desktop-as-a-Service (DaaS).

Virtual desktop instances (VDIs) and similar services are growing in popularity since having your computer power in the cloud is a great way to keep maintenance costs down and centralize all trouble-shooting.

Phones

So you have your users in touch with their applications, right? Now you need them in touch with customers and vendors. Smartphones are integral to getting business done and that probably won't change anytime soon.

Most businesses don't need a ton of features when it comes to phones, but it's important to understand your needs. For example, perhaps you need your users to be able to transfer a call, receive voicemail, place customers on hold, and possibly have an auto-attendant.

The good news?

Most of these devices are pretty standard across most platforms. As a cloud enabler, here at EnableIP we're a big fan of hosted VoIP solutions. They decrease your exposure to hardware failure and let you take advantage of the provider's redundancy. Most of these providers offer a 99.999% up-time guarantee, meaning that reliability isn't a concern. (Keep in mind, however, that your own WAN has to be up to use this solution.)

Here's more good news:

Most VoIP providers offer the physical phones dirt cheap or free. While at first they may try to sell them to you at full price, with a little bit of haggling (or getting competition involved) you can usually secure free phones — or damn close to it.

Key Takeaway

Every business has different needs. When it comes to connecting your locations to the internet, to each other, and your users to their applications, the information provided above is the foundation that you can build upon.

It's important to consider where your company is now, and where it will be in 2-3 years — then build an environment that's ready to scale. As the saying goes, "Strike while the iron is hot."

If you get the opportunity for rapid expansion, you don't want to be held back by your technology — especially in an age where scalability in technology is incredibly easy as long as you do some legwork early on.

About Enable IP

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 Enable IP 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.

Enable IP
WAN UPTIME EXPERTS