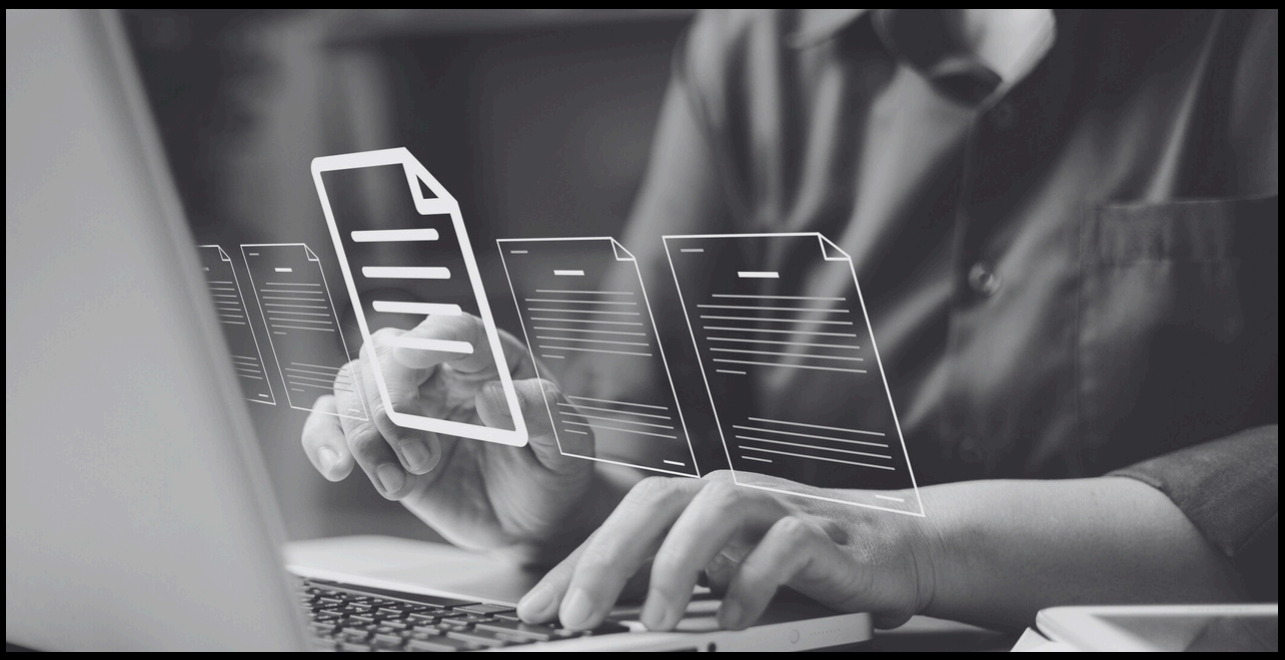
WYRE TECHNOLOGY



3 COMMON NETWORK PROBLEMS

wyretechnology.com

Contents

Introduction

Your network is the backbone of your business—from sending emails and accessing cloud apps to hosting virtual meetings and securing sensitive data. But when that network starts to hiccup, so does productivity.

Even minor problems—like lagging Zoom calls or a printer that suddenly disappears—can be signs of deeper issues. And if those issues go unchecked, they can lead to costly downtime, security risks, and frustrated employees (and customers!).

The good news? Most network problems fall into a few predictable categories.

In this e-book, we break down three of the most common challenges we see across industries: weak Wi-Fi coverage, outdated (or downright ancient) components, and a lack of proper network segmentation.

Whether you're managing a growing nonprofit or leading IT at a multisite manufacturer, understanding these core issues—and knowing how to fix them—can keep your business connected, secure, and running smoothly.

Common Network Issue 1

Weak Wi-Fi Coverage

Have you ever been in the middle of an online meeting and watched in nervous confusion as the image on the screen starts to fragment or the speaker's words go out of sync?

If this happens with most meetings, most times, then your Wi-Fi signal isn't strong enough to handle the load from your network.

Wi-Fi begins at an access point, or AP. An AP allows other wireless devices to connect to a wired network. The AP then gives all the devices connected to it access to the outside world (i.e., the internet).

If your Wi-Fi signal is weak, the nearest AP is a good place to start troubleshooting.

1.1 : Are Your APs Undersized?

The number of devices on your Wi-Fi network matters.
More devices means higher demand.

For example, a nonprofit with four desktop computers, one server, and one printer would need a simple, straightforward network.

On the other hand, a utility company with thousands of devices would have to scale up in a serious way to include dozens of segmented networks and an array of components.

If your business has grown since your network was installed, it's time to take a fresh look at your components—including any APs—and make sure they're still the right fit.

Remember: having the right components for the size of your business helps more than just the Wi-Fi signal. It can also improve stability and security.

1.2 : Is The Nearest AP Too Far Away?

Walls, closets, cubicles, metal, other Wi-Fi devices, even water coolers—all of these can cause a drop in your Wi-Fi signal quality. Be sure APs are well-placed to provide service to the necessary areas and are kept away from obstacles that might cause interference.

If you're a small-to-medium-size business, or SMB, look into an affordable, high-performance product like Ubiquiti's U6 line of APs, all of which can be ceiling-mounted, providing a clear path for your Wi-Fi signal.

1.3 : Do Your Components Need Updates?

When was the last time the firmware on your network components was updated? Manufacturers provide downloadable updates at regular intervals, and if the updates aren't installed, not only will your components not work as well, but they also may be vulnerable to cyberattacks. In fact, according to Gartner report, "By 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability."

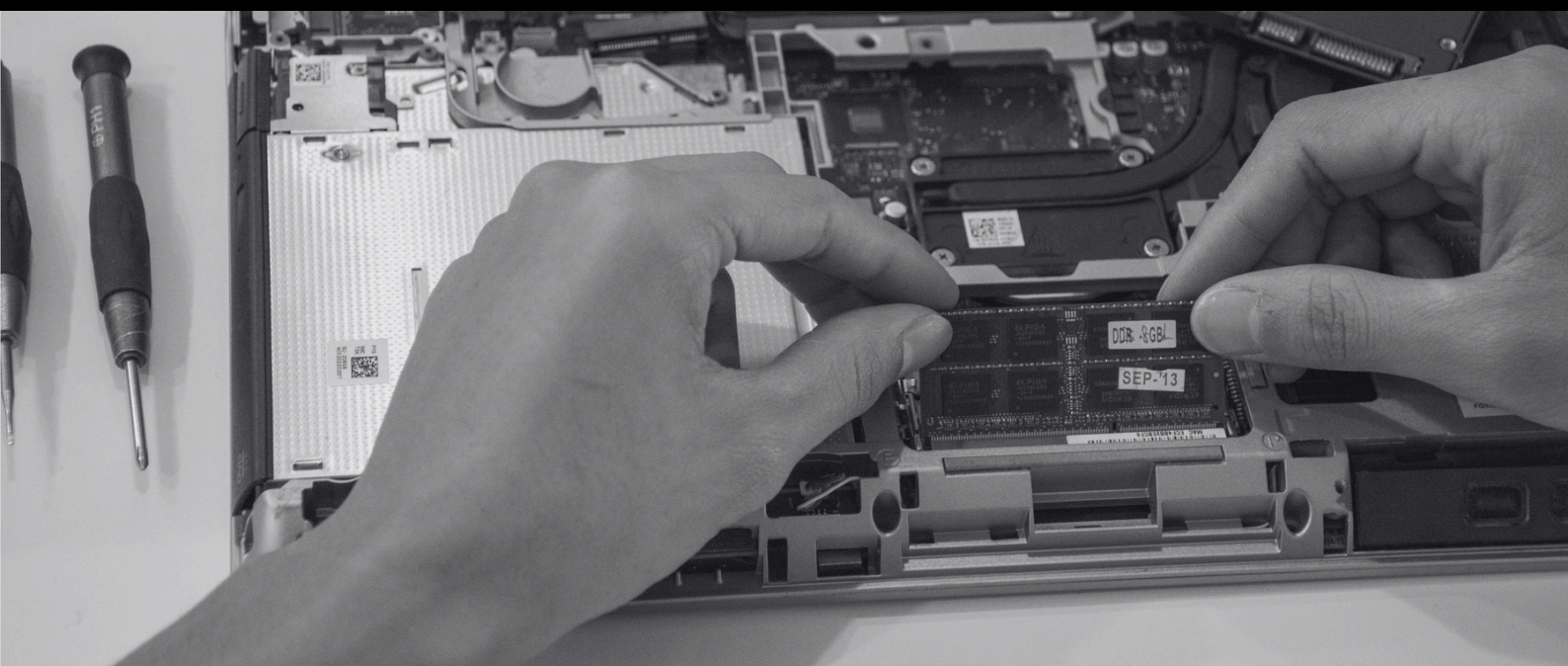
Installing firmware updates is simple (though it's best to perform the installation after a full backup and when the least number of users will be affected). Again, check with your product's manufacturer for instructions.

1.4 : Do Your Components Need *Upgrades?*

How old is your router? Your switch? Your AP? What's the state of the wiring that connects them?

If you're still using the same computer components from five years ago, they're probably in need of replacing. Technology moves fast.

Curious about how easy—or not—it is to upgrade older components? Keep reading!



Common Network Issue 2

Legacy Systems

If your company has been around awhile, you're probably familiar with the term *legacy*. In computing terms, legacy refers to older, outdated, no-longer-supported software and hardware that's still in use by a company.

As you can imagine, legacy systems have their downsides. In 2020, technology market researchers Vanson Bourne conducted a survey called "The State of Data Management." They spoke with 500 IT decision-makers in both the US and UK. When discussing legacy environments, 88% said their business had experienced "challenges trying to load data into data warehouses [management systems for data]."

One of the biggest reasons for the challenges? Legacy technology.

And for 49% of the survey's responders, legacy systems were "restricting data movement and the loading of data into a data warehouse."

Difficulty moving and managing data is bad enough, but perhaps the biggest downside to a legacy system is its vulnerability to cyberattacks.

Security patches for out-of-date software and hardware don't exist—when the equipment is stamped as "end of life," or EOL, companies stop supporting it. This gives cybercriminals an easy target. In 2020, Rangely District Hospital in Colorado was targeted by a ransomware attack. The breach may have included confidential patient information, such as social security numbers, driver's license numbers, health insurance details, and even diagnoses.

The attack targeted the hospital's legacy software system, leaving staff unable to view patient records.

In 2020, Adobe-owned e-commerce platform Magento was targeted by cybercriminals. Using malicious code, they stole customer credit card information. The malware infected 8,170 stores across all platforms, and "82% of stores that had malware were running an unsupported version of the product."

Magento's legacy software was out of date by only a few *months*.

2.1 : Why Companies Use Legacy Systems

Even with all their potential problems, legacy systems are used for a reason—several, actually—especially by established businesses.

- Legacy systems can be critical to a company's IT infrastructure. Banks use legacy environments to process transactions and manage accounts. Branches of the US government, like the IRS, are steeped in legacy systems. And retail merchants report spending "58% of their IT budget to maintain legacy systems."

- Legacy environments are familiar. They've been in use for a long time, and staff know exactly how to finesse the systems to get what they need.

- Legacy products seem cost effective. After all, you're simply paying for upkeep, right?

Not quite.

Yes, upgrading a legacy system can be costly: new products and equipment, installation, licensing, plus training staff to use the new system.

But not upgrading brings its own set of problems.

2.2 : Problems with Legacy Systems

- Parts for legacy systems are expensive. According to the US Government Accountability Office, "Ten critical federal information technology (IT) legacy systems . . . ranged from about 8 to 51 years old and, collectively, cost about $337 million annually to operate and maintain."

- Recruiting support is difficult. Finding specialists familiar with legacy systems can be challenging, not to mention costly.

- Legacy systems use more power than modern systems and therefore have a bigger carbon footprint.

- Legacy equipment is slow. In fact, since 2013, supercomputers have increased in speed by 40% every year.

2.3 : How to Migrate from Legacy Systems

Moving away, or migrating, from a legacy system may not be as difficult as you think. There are two main paths: transformation and lift-and-shift.

- Lift-and-shift moves your network's software and data to a cloud or hybrid-cloud service—with little-to-no redesign.

- Transformation, or modernization, slowly and methodically brings your network software and hardware up to date with current technology.

No matter which path you choose, it will take time and planning. But it *is* possible. The details will need to be worked out by your CIO and technology team. If you're a small business, or you don't have in-house IT staff, contact your MSP for help.

Common Network Issue 3

Lack of Network Segmentation

Segmenting a network divides it into separate sections. This is accomplished via switches. A switch's job is to allow multiple devices—from printers to servers to tablets—to see and talk to each other.

Network segmentation is an important—and often overlooked—way to protect your network from cyberattacks. When the network traffic, or data, is isolated between segments, with firewalls for added security, those segments become your front line of defense against outside cyberattacks. How? Cybercriminals who sneak through the first line find it harder to get through the second.

Different security rules can even be created for each segment, ensuring each group of users has only the permissions they need to do their job. This helps contain malicious attacks and can prevent untold amounts of damage.

Network segmentation is best handled by your IT staff or an MSP.

Conclusion

No matter the size of your network, there will always be issues—from outdated components to security vulnerabilities. This means every network needs some kind of support. After all, you likely already wear a number of hats. IT doesn't have to be one of them.

If you don't currently have an in-house IT team, research MSPs in your area. And if you're in Chattanooga, Tennessee, or anywhere else around the world, WYRE always helps.

Looking for a second opinion?

Get a free consultation with one of our experts!

WYRE ALWAYS HELPS.


423-874-8230


wyretechnology.com


solutions@wyretechnology.com


@wyre-technology