



Uptime Comparison of Web-based vs Client/Server Systems

“What if the web goes down?” It’s a common question when people investigate web-based solutions. Certainly, technology introduces different failure modes than traditional processes. This begs the question, “How reliable are web-based solutions when compared with their client/server counterparts?”

The short answer is that web-based dental software applications, properly hosted, will be about ten times more reliable. Let’s now explore what drives this amazing reliability. We will also identify some actions that can mitigate the small risk associated with web availability.

Client/Server vulnerabilities

“Can you call back? Our server is down.” It’s almost a cliché. It happens with such regularity that we just take it for granted that it is just a fact of life. Many offices have grown accustomed to this situation as part of life with dental software. It is so commonplace because client/server based systems have many points of failure and any one of them can bring the whole system down.

Most client/server failures can trace their cause to two primary origins.

First, typical client/server installations are not redundant, nor are they fault tolerant. There are many potential single points of failure in a client/server setup. It is like a long chain where the strength of the whole is only as strong as its weakest link. When one link breaks, the whole chain is rendered useless. Every hardware component found in the server (motherboard, memory, hard drive, communications cards, etc.), the software installation and drivers, they all are potentially catastrophic failure points.

One solution is to use “fault tolerant” architectures, systems and equipment. Though it’s a nice theoretical option, it’s just not practical for a dental office to implement. Fault tolerant systems are so expensive that just the purchase price will break the budget. Additionally, they require some real smarts to put them together and maintain. (Not that dentists aren’t smart. They are smart, just in a different area.) It is a given fact that all computer hardware will break sometime. Computers (even really good ones) are complex electronic machines that will fail. If failure of a computer (or one of its components) is a given, then the ideal solution is to create an architecture that accepts that and designs for it. Unfortunately, there is no such architecture available at a reasonable price for office based client/server systems.

Secondly, the typical office based client/server installation is put together using consumer grade equipment, processes and environments, and is maintained in a very haphazard way.

Think for a second where the typical server is located. Is it in a climate controlled, sterile Network Operating Center (NOC)? Or is it in a broom closet next to the detergent and mop? Fundamentally, the typical installation of a client server based system is inherently at a disadvantage, simply by reason of where it is installed and how it is configured. The risk of bumping, or spilling, or nudging, or moving is synonymous with the risk of failure. Even just the extra humidity found in some offices or regions can significantly reduce the life of computer components. And guess what; the opposite is also true. Too little humidity creates a static environment that is a death sentence for any computer. Either way, if it’s not “just

right” problems are more likely. Even with a perfectly controlled environment, things still break.

Finally, when a client server based system goes down, you will need to call your “IT guy” to come to the office and help get it back up and working. Sometimes all it takes is a “reboot”, but more often than not, there is an underlying problem that needs fixing. Besides the financial consequences of the IT bill, the service call can take a valuable time. Even with responsive service, you still are looking at hours; for typical service it can be days or longer.

The result of all these failures ends up as system downtime that is measured in hours per month or days per year. That quality of service is very costly and is far inferior to web-based systems.

Web-based systems

Web based systems will typically have downtime that is measured in minutes per year. In fact, quality web-based products spend less down time than is typically required to reboot a windows PC once a month. Why is this? There are several reasons.

Redundant and fault tolerant architectures. Web-based systems are frequently developed using fault tolerant and redundant architectures. These setups assume that every component will break sometime. So, the architecture accommodates for the equipment to break. Think of it like the backup systems found on the Star Trek Enterprise. It seemed as if every episode some Klingon ship was pelting the Enterprise with photon torpedoes and lasers; but because the ships architecture had been built to anticipate system failure, it was ok. Backup systems and secondary backup systems were in place to take over for the failed primary system. And it did this on the fly – no downtime, no peril (well, maybe a little peril – but it wouldn’t be much of a movie if there weren’t a little peril).

Professionally housed, managed and maintained systems. There is something really comforting to know that really smart people are watching your system on a 24/7/365 basis. Literally, with professionally managed web-based systems there is someone who is on guard, watching the process and functionality of the hosted system on a continual basis, even after you go home at night, and even on weekends and holidays. Because someone is watching the system statistics, they can tell if a hard drive is starting to spin a

little slower, or if a CPU is heating up more than expected. Hardware will usually give some sort of a warning before it breaks completely, and these variant components are replaced routinely before they fail.

Hardware Maintenance. Many hardware components have published useful service lives or quality guidelines. When the published service life of a hard drive or other system component is up, or it no longer works within the service guidelines, it will be replaced, even if it is technically “still working”. In a typical dental office, the old component will just stay in the machine until it breaks. (remember that “weak link” discussion?)

Hot swappable. Many industrial components in professionally managed environments are “hot swappable”. This means you don’t have to shut down the system to replace the component. So, if a power supply on a server starts to go bad or completely fails, or if a hard drive stops working, it is taken out of the computer while the computer is still running, and is replaced on the fly. The computer does not need to be turned off to replace the component. It’s sort of like being able to change a flat tire without having to stop the car. Pretty amazing stuff, but that’s what you get with a redundant web-based architecture.

Controlled environment. Sterile, humidity controlled environments are made perfect for the operation of computers. It’s sort of like the Bahamas of technology. Think of the perfect Caribbean vacation weather. Sunny, a little breeze, a shade tree, no insects, etc. Well, that’s what a Network Operating Center is for a computer. Professionally managed web-based systems are housed in Tier 1 “hardened” Network Operating Centers (NOC’s). This type of environment lengthens the life of computer components. It’s good for quality service, and it is also good for the NOC – they don’t have to replace broken hardware as frequently. Everybody wins.

So, what if the web does go down?

We’ve covered pretty well why web-based offerings can have substantially better uptime, but does that mean they are infallible? No. No more than you can guarantee that the power won’t go out in your office. Sometimes construction will cut the network line to your office, or a glitch at your Internet

Service Provider (ISP) causes a stoppage in service. What can you do then?

The most common method of protecting against a web access failure in a dental office is to bring in a redundant web access point. A common and simple method is to have a Verizon or Sprint wireless network card on your network in case the neighbor's backhoe didn't call Blue Stakes first. It comes with a monthly charge, but some offices find that the security of knowing they have an alternate web access point is worth the \$50 per month fee.

Many offices that start on this type of redundancy find that after many months or years of uninterrupted service, they choose to go without the redundant web access point. Actually, the risk is substantially less than you would think.

Utilities are more reliable than private services.

In addition to the inherent vulnerability of a client/server based system, they are also vulnerable to loss of electric power. The same goes for web-based systems.

If the power goes out and your computer system won't run, then you probably are also having a hard time running your air compressor, autoclave, lights, etc. So, power is not just a technology problem

This risk can be mitigated by the use of Uninterruptable Power Supplies (more useful for "brown outs" than actual power outages), or by external generators for more extended periods of time. So, how many offices purchase a generator to protect against a loss of electric power in the office? Not many. Why? The answer is pretty simple.

Electric power is a public utility. As such, when an outage happens, there are typically hundreds or

thousands of others with the same problem. With many people all experiencing the same failure, the company will put all available resources on the problem until it is fixed. These outages, in most areas, do not last very long, nor do they happen very often. If you live in an area that does experience frequent and prolonged failure, then you are probably among those who have a generator.

The same principle goes for internet access and internet service providers. If the internet goes down, there are hundreds or thousands of others in the same situation. The local internet service provider puts all available resources at the problem until service is restored. Because you are not alone, the problem is resolved much quicker and at less expense.

So, most offices find that although the internet does sometimes go down, it is so infrequent and of such short duration, that a backup internet access point isn't justified. Client/server system downtime is on the order of ten times as disruptive in both frequency and duration when compared with web-based solutions.

In conclusion

Though it's a reasonable question, "what do I do if the web goes down", the facts indicate that the web will be available much more consistently than your in-office server will be.

If you live in a particularly vulnerable location or if your practice justifies the additional \$50 per month, you can completely protect yourself from internet outages with a simple wireless internet service from the major phone companies.

About Curve Dental

Curve Dental is a dental software company that delivers practice management solutions via the web. Our customers can schedule, invoice, manage recall, manage insurance, chart, and much more using only a browser and Internet connection. If you can bank, shop and book a vacation online, why can't you manage your practice on-line? When it comes to web-based dental software, Curve Dental leads the way with simple technology and impeccable customer service. For more information visit www.curvedental.com or call 1-888-910-4376.