

By Erik Eckel

Microsoft hit a home run with Windows Small Business Server. It's becoming increasingly difficult to find small business servers not running the economically priced Windows operating system. The Windows Server 2003 platform provides stability, while the Exchange and SQL engines provide scalability. Wizards, meanwhile, simplify administration. When deploying Windows Small Business Server, or any small business network, most every implementation is optimized if you keep the following 10 elements in mind.

1 Servers aren't always necessary

AMI Research reports that of 68.5 million small businesses worldwide, more than 21 million have multiple PCs but no server. That figure can be found in Microsoft promotional materials designed to help IT consultants understand the small business space and sell servers. But the fact is, many organizations don't have servers because they don't need them. Other organizations have servers because an IT professional or consultant sold them one, but they don't actually require it.

I've encountered customers whose previous IT consultants sold them \$4,000 servers (with dual-Intel Pentium CPUs, no less) that do nothing but fulfill DHCP services. That's a waste. While technology professionals should always work to deploy the best technologies for clients or organizations in which they work, IT pros have a responsibility to ensure the correct technologies are deployed.

If a company employs fewer than 10 employees and isn't forecasting aggressive growth, it's likely a peer-to-peer network of Windows XP Professional systems will meet the organization's needs. Should the organization grow, the investment in XP Pro systems can still be leveraged. When exceeding 12 or so employees, though, organizations are typically better served with a server.

One easy but all-too-common mistake is easily avoided. Never deploy Windows XP Home systems in office or business workgroup environments. The consumer OS doesn't offer the security controls Windows XP Professional boasts, nor can Windows XP Home join a Small Business Server-powered domain (should the organization grow to the point that it requires centralized administration).

2 Good topology is planned, not accidental

Poorly configured networks are everywhere. The number of three- and four-hop networks I encounter as an IT consultant is mind numbing. Adding four- and five-port routers/switches here and there isn't the proper way to connect networks. Although it's an easy approach, performance inevitably becomes a problem.

Thus, it comes as no surprise when a small business with nine systems and four switches approaches me complaining of poor network performance. Worse yet, many of these networks often possess multiple 192.168.x.y and 10.0.x.y subnets.

Replacing three four-port switches with a single 16-port switch typically introduces dramatic performance improvements. Even with only 10 or 12 employees, the additional ports often prove handy for providing a single interface for all client systems, a server if it's present, and firewall and DSL or T1 connectivity.

It's easy to fall into the trap of simply adding switches as a network expands, but before you add a second switch, plot the network on paper. Count the number of hops a connection must navigate before reaching the gateway. Often, you'll find investing in a few extra cable drops (to avoid requiring an additional switch in a quickly expanding office) provides performance gains that more than justify the expense.

Whenever you prepare to add new systems or are prepping a new network, consider its topology carefully. Work to minimize the number of hops data must travel, even if investing in a switch with more ports or new cable drops is required.

3 Network equipment deserves investment

The average lifespan of a network switch or firewall is probably four to five years. Others may tell you three years is the average, but let's be honest--most everyone tries to maximize their investments by running equipment longer.

If you try to save funds by purchasing cheaper network equipment, you'll almost certainly pay the price down the road. Less expensive switches, firewalls, VPN appliances, and routers are available, sure. But they're made with lesser quality materials. That means the power supplies are less robust. Ports are more likely to fail. Cheap fans are more likely to malfunction, thereby resulting in failure due to overheating.

When designing or re-architecting a small business network, budget funds appropriately for commercial-class network equipment. Buy the best the organization can afford. Although there are no moving parts, and the equipment is likely parked in a closet where no one will ever see it to appreciate it, most every aspect of an organization's data and communications will run through the equipment. If there's ever an element that justifies purchasing quality components, that's it.

4 IP addressing deserves attention

Just as a network's topology deserves attention and planning, so too does a network's IP addressing scheme. The popularity of universal threat management (UTM) appliances and proprietary router and firewall operating systems, such as those found in Cisco, SonicWALL, and other companies' devices, often introduces a variety of operating subnets.

As a result, troubleshooting connection failures, performance issues, and other problems is made exponentially more difficult. Instead of maintaining three different subnets, or worse, encountering multiple DHCP devices serving up the same IP addresses within the same ranges (don't laugh, it happens), always plot network topologies and the corresponding IP subnets on paper. A world of mistakes (and hurt) can be easily avoided, as discrepancies are easily spotted when a network is properly documented on paper or within Visio.

Multiple subnets aren't always bad, of course. Occasionally, a small business may require two subnets. When security is of particular concern, maintaining sensitive data on a secondary subnet available only to limited personnel (and typically removed from wireless connectivity) may prove best. Such secondary subnets also prove helpful when you want to limit VPN or remote traffic to specific network segments.

5 You should choose internal domain names carefully

The Microsoft community recommends rolling out servers using the .local domain. The problem is that Macintosh systems encounter trouble resolving addresses with Active Directory when the .local domain is used because Apple's own Rendezvous technology was designed to use the .local namespace.

If an organization doesn't need to include Macs on its network and never will, the problem's likely not an issue. But if Macs are to be present at any point, selecting a different namespace will help avoid having to make other changes to enable the Apple systems to properly resolve DNS requests.

That said, you should also guard against using publicly routed domain names as an internal domain namespace. Several years ago, I made that mistake on a test system, and multiple issues arose due to trouble resolving DNS requests. User logons sometimes took 12 to 15 minutes to complete. Design networks to use top-level domains that aren't publicly routed on the Internet.

Many administrators prefer the .local or .lan top-level domains. For testing purposes, the .test domain works well. The .example domain, meanwhile, is a safe, if unsavory, bet.

6 Data requires segregation

When designing a small business network, plan on separating the network's data to maximize data protection, backups, and recovery.

How? Follow the best practice of installing an operating system's files on a different partition (and preferably a different hard disk) than that housing user and application data. Better yet, ensure a Windows server's Exchange database is parked on its own partition or disk, too.

Ultimately, that's a lot of partitions and disks. Most small businesses are unlikely to maintain the three (or six, if disk mirroring is implemented) hard disks such planning requires, but at least give it some thought. Organizations unable to maintain (due to cost restrictions) separate hard disks for an operating system's files, user data, and the Exchange database should place that much more emphasis on making sure that backup operations properly complete on a regular basis.

7 Wireless technologies are problematic

Although they're full of promise, wireless networks frequently prove frustrating, introducing problems like security vulnerabilities and flaky network connections. From relatively weak WPA keys to easily defeated MAC filtering, wireless security (or the lack thereof) is infamous. Tack on reduced throughput, the need to position antenna and access points carefully, and the potential for introducing yet another routing device serving potentially conflicting IP addresses, and you may be prompted to rethink whether wireless access is really required on a network.

Certainly, occasions will arrive in which an organization's users require the mobility wireless networking provides. Or a business may occupy a facility in which running required Ethernet cables simply isn't viable. When designing or planning such networks, be sure to seek routing equipment that also includes wireless service. By combining routing/firewall/VPN features and wireless connectivity in a single device, some of the routing issues that arise when adding multiple devices to a network can be eliminated (although you're still stuck with many of wireless' security headaches).

8 License planning is critical

Planning peer-to-peer workgroup licensing requirements is simple. Purchase as many systems running Windows XP Professional as you require and roll them out.

Planning Small Business Server licensing requirements is another matter. Windows SBS ships with just five client access licenses (CALs). Unlike other Windows server platforms, the user CALs associated with Windows Small Business Server cover all SBS' technologies, including Exchange and SQL.

Although that's relatively simple, there's still some confusion regarding the two types of SBS CALs available: User CALs and Device CALs. Choose User CALs if you wish to tie licensing to individual users; select device CALs if you wish to tie Microsoft licensing to servers and PCs (such as when you have multiple shifts of call center or customer service personnel using the same PCs throughout a typical day).

SBS ships with five user CALs and you can buy additional CALs in sets of fives and tens. But once you hit 75 users, you're done. If you anticipate exceeding 75 users anytime in the foreseeable future, you should begin making plans to migrate to a standard version of the full-blown Windows server platform instead.

9 Terminal Services changed in SBS 2003

Terminal Services licensing changed with the introduction of SBS 2003. Small Business Server 2000 supported Terminal Services running in Application Mode, but SBS 2003 does not. What's that mean?

If users must access network applications powered by the server, organizations should design their small business network to use Windows Server 2003 instead. Only users possessing administrator rights can log on remotely to a Windows SBS 2003 desktop and even then, SBS 2003 supports a limit of two such concurrent sessions.

Microsoft claims Terminal Services in Application Mode was disabled in SBS 2003 as a security precaution. As mentioned previously, however, the feature is still available in Windows Server 2003.

Ultimately, your best bet when designing a small business network is to limit as many remote connections as possible. But should your organization require such connectivity, be aware that SBS 2003 may not meet your requirements.

10 Review features-versus-needs before purchase and deployment

This most important step is often forgotten. Planning discussions almost always begin with an energetic needs assessment. But technology professionals servicing smaller organizations often leave such planning meetings to begin ordering equipment and coordinating a resulting migration or rollout.

Once discussions of IP addressing schemes, Active Directory configuration, Exchange administration, performance reporting, and the like begin, it's easy for technology professionals to lose focus and forget business requirements.

For example, business owners may be focused on adding the ability for traveling employees to securely access sensitive resources while on the road via VPN. Or they may be eagerly awaiting the opportunity to integrate user administration, file and print sharing, e-mail, and Web hosting on a single system in-house.

If the technology professional doesn't design the small business network to power the services the business demands, the table is set for disappointment. It's easy to forget to design the network to support secure VPN connections or to specify the proper IP address necessary for Exchange e-mail and Web hosting once you become wrapped up in the many other details that inevitably accompany such a project.

When designing a small business network, between discussing the organization's needs and announcing the resulting solution, technology professionals would be wise to schedule an extra meeting. The purpose? To ensure the proposed solution and new network design not only possess the capacity and features required to meet the organization's business requirements, but to confirm that the new network will be implemented in a manner that maximizes its capabilities and enables users to meet the organization's business requirements.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) [XML](#)
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Administration NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["10 things you should know before deploying Microsoft Windows Small Business Server 2003"](#) (TechRepublic download)
- ["How do I... Manage Microsoft's Windows Small Business Server 2003 e-mail accounts"](#) (TechRepublic download)
- ["10 things you should know about Windows XP Backup"](#) (TechRepublic download)

Version history

Version: 1.0

Published: September 25, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team