CHAPTER 2

SMB Networking Environments and Solutions Design Considerations

The past two decades saw the commoditization of computer networking in the small-medium business (SMB) arena. In 1980, DEC, Intel, and Xerox (DIX) published a document known as the "Ethernet specification," the "Ethernet version 1," or the "Blue Book." In 1982, that document was updated to Ethernet Version 2. Espec-2 remains a valid and relevant standard even now, but it is much easier to set up a computer network today than it was back then.

Think for a moment about the networking hardware used in the early 1980s: 10 Mbps shared media, network interface cards (NICs) with external transceivers, vampire taps, thick coaxial cable, and repeaters to extend the network topology. In terms of networking operating system (NOS) software, think of minicomputers or mainframes; there were no viable network operating systems for PCs in 1982, although fledgling efforts were under way to develop them.

Add to those mental pictures (if you can still imagine them) PC platforms equipped with a whopping 640 KB or 1 MB RAM and CPU clock speeds of 4 MHz. You are now on the cutting edge of networking and PC computing of the early 1980s! And the aforementioned items were not available in office supply stores or online. Why? For the simple reason that in 1982, even though the precursor of the Internet (the ARPANET, developed by the Advanced Research Project Agency [ARPA] in 1969) was in existence, today's web-oriented Internet, which, using TCP/IP protocols, allows us to make online purchases with a click of a mouse, was not. In addition, the high cost and limited availability of networking and computing products in those days did not make them viable candidates for the shelves of office supply stores.

Fast-forward more than a couple of decades to today. Networking products like 10/100/1000 Mbps NICs, hubs, routers, switches, relevant cabling, firewalls, and plentiful high-performance PC hardware and software are commodity items. They are available at many types of brick-and-mortar outlets, from electronics stores to office supply stores to regular department stores. In addition, hundreds if not thousands of other networking products from numerous vendors (both hardware and software) are available at online stores and Internet auction sites. These products range from basic equipment that is applicable for home networking to complex multiservice devices and software applications that support the operations of even the largest of enterprises. Given the fierce competition in the networking field, many Internet sites specialize in providing price comparisons to allow

potential buyers (from home users to SMBs and large enterprises alike) the option of purchasing a desired product at the lowest possible price.

One thing is certain: Wide availability of networking products has made them affordable (and indispensable, it is probably safe to say) to support the endeavors of every business category, including all sizes of SMBs. Many of the currently available networking products are also easy to use and to install, especially when they are deployed individually or in smaller networks. The network equipment vendors (including Cisco) are to be congratulated for making networking hardware and software easier to use.

At the same time that ease and simplicity have been prevailing for home users and small office/home office (SOHO) users, there has been a growing diversity and an increase in sophistication and capabilities of the networking gear, software, and business solutions meant for SMBs and large enterprises. Take IP Telephony, for example. All of the IP Telephony solutions operate over a data network (packet-switched) infrastructure and can nicely integrate with the circuit-switched legacy installations. Consider that telephony has been evolving for more than 100 years. Porting the existing telephony features, adding new ones, and providing for integration of IP Telephony with the existing telephony systems implies a degree of complexity and sophistication that is not exactly a "plug-and-play" operation yet. Progress is continuous, though, and even as this book is being written and released, Cisco and other IP Telephony vendors are crossing the technical chasms. IP Telephony solutions are discussed in more detail in Chapter 8, "IP Telephony Solutions."

When you combine the increasingly growing intelligence and capabilities of the networking equipment with the diversity of the SMB landscape, as discussed in the next section, it becomes advisable for anyone designing a network to adhere to a principle that seems to have withstood the test of time: Effective computer networks and networking solutions cannot be slapped together without going through a design process. If you do not follow this principle, the potential is too great for underutilizing the network capability and having an SMB operate in a reactive mode with the limitations and quirks of the poorly operating network driving business decisions rather than supporting them. Computer networks and networking solutions need to be designed and implemented to support the business and its mission instead of businesses barely making it or going under because of their networks.

One Name, a Multitude of Shapes and Sizes

Trying to fully categorize and analyze the SMB market might best be left to the market research firms, the Small Business Administration (SBA) in the United States, or the equivalent government institutions in other countries. Suffice it to say that it is hard to get out of bed in the morning and get through a day without numerous encounters with SMBs. Even though some businesses you encounter might seem to be large enterprises, from the perspective of designing a networking solution, those enterprises are composed of smaller units that effectively function as SMBs that are integrated with a high-capacity, high-performance core network architecture that a single SMB might not require. Effectively, on

the edge of a network, even the largest of enterprises, regardless of its sector, size, or shape, can be thought of as an SMB. And even though networking solutions need to be tailored to support each SMB sector and size category, a commonality of the networking infrastructure and solution functions applies to the entire SMB landscape.

Business Sectors

SMB sectors span the alphabet, from automotive dealers through zipper repair shops and zoos, including everything in between: education, travel, health care, finance, legal, delivery, entertainment, food services, manufacturing, transportation, and real estate, just to name a few. These businesses serve the varied and ever-evolving needs of the societies that we live in, but at the same time they share three common fundamentals: They all offer a product or a service to a group of customers; they all have to remain competitive and fiscally responsible if they expect to survive and to prosper in the marketplace; and, generally, they all are working toward a certain goal. In for-profit organizations, the objective is most often profitability; for nonprofits, the goal is to offer a valuable service or a product that a society has deemed worthy of not being subject to taxation.

All SMBs, regardless of the sector in which they operate, rely on utilities that are now routinely taken for granted in a modern society: electricity, telephone service, running water, or physical mobility through a well-established transportation network. Computer networking has not been around for as long as electric service, telephones, or divided highways, but from my perspective, it is well on its way to becoming one of the common utilities. Consider electricity. Numerous appliances performing a seemingly unimaginable number of functions plug into standardized electric outlets to support the complex requirements of our lifestyles. Consider a well-designed computer network. Well, we are not quite there yet (being able to plug several different devices into the network and having them work instantly), but progress is heading in that direction.

A well-designed network should transparently support a wide range of business applications to advance the varied missions of SMBs and other enterprises, regardless of their size. Certain generic applications—such as payroll, billing, accounts receivable, or electronic mail—are common across all of the business sectors, although their specific features vary as a function of the size of the enterprise that they support. Other applications are unique to each sector, including specialized banking software, inventory control for retail outlets or wholesale distributors, automated production controls in manufacturing facilities, or custom programs that access patient databases in health care facilities. Often, the effective use of these unique applications ultimately offers an SMB a competitive edge and supports the fundamental business mission of delivering value to customers.

Consequently, when designing an SMB networking solution—subject to the design guidelines discussed in Chapter 1, "Effective Networking Solution Design Process"—it is important to keep in mind the ultimate goal that the solution will support, regardless of the business sectors that SMBs find themselves in. Supporting existing or future applications is, needless to say, extremely critical. A security solution is necessary to protect the effective

functioning of the business applications and the attendant information that they generate. But remember that although a security solution might appear attractive in and of itself, to be effective and useful, it must integrate well with the existing applications. If this sounds like an implementation rather than a design issue, keep in mind that the line separating the two is often thin. That is true especially in the minds of stakeholders, who have a keen interest in the final outcome of a solution rather than in maintaining a technical separation between the two stages (design and implementation) relating to a solution's deployment.

When it comes to the design and implementation stages of a networking solution project, careful management of stakeholder expectations is critical when a proposed solution is a replacement for something already in existence. Consider IP Telephony, for example. If you are considering a brand-new telephony deployment, chances are that IP Telephony solution(s) will win compared to their circuit-switching siblings because IP Telephony solutions facilitate effective and inexpensive business communications.

However, because telephony has been around much longer than computer networking, IP Telephony solutions will more than likely replace or significantly upgrade the existing telephony infrastructure. The SMB might be willing to live with the limitations of its existing installation if a significant investment in it has already been made that would have to be scrapped to proceed with the new solution. Thus, deploying a brand-new solution is quite different from replacing an existing, functioning one. During the design stage, the issue of implementation needs to be considered in much more depth for significant upgrades or replacements than for a brand-new deployment. This principle applies across all business sectors and sizes.

Business Sizes

From the point of view of designing a computer network or a networking solution, the business size influences the quantity of equipment, the level of its performance, the layout or network topology, and the interconnections between the networking equipment. Business size should not necessarily affect the type of functions that a network offers.

At a minimum, basic functions for the network in any size business should include the following:

- Internal and external connectivity for resource, file, and database sharing
- Support for common and specialized applications
- Security

In environments with existing legacy networks, you always need to ensure interconnection with legacy equipment and support for legacy applications. The business size might well determine the following:

- Whether the typical three layers (access, distribution, and core) are going to remain distinct or be collapsed into one or two layers

- Whether a single integrated appliance will be able to accommodate the relevant business needs (LAN/WAN connectivity and security, for example) or whether discrete devices optimized to perform routing, switching, or security functions are required

Consider a small office with a dozen or so employees occupying a fraction of a large office building. Then consider an enterprise with thousands of employees occupying several office buildings. What is the difference between these two environments from a network solution design point of view? Think about modularity and scalability. In every product category—whether it is routers, switches, firewalls, or telephony solutions—Cisco offers a scalable spectrum of products to accommodate a spectrum of business sizes. At the lower end of the spectrum, the approach might be to use fixed configuration and/or integrated products. Refer to Chapter 5, "Cisco Security Solutions," for a discussion of the spectrum of security products and solutions.

As you progress through the SMB size scale, a modular design approach using specialized blades that support routing, switching, security, or IP Telephony from a single chassis becomes more preferable and cost effective. A larger SMB size translates into higher capacity and higher port density on fixed-configuration switches or on blades for modular switch units, routers that switch more packets per second, or firewalls that support more simultaneous connections. Modularizing the SMB or even a larger enterprise into distinct units, applying appropriate product categories to those units, and integrating those units via a logically hierarchical topology is a key concept in designing scalable solutions for SMBs of varying sizes.

Business Missions

A business mission, often nicely framed and gracing the walls of the business establishment, proclaims the reason that a particular business exists. It might take a creative imagination to establish a connection between a business mission and a router, a switch, or a firewall humming along on a rack in a telecom closet, a data center, a dusty crawl space, or perhaps even under someone's desk. However, if you choose to accept the premise that a computer network is becoming as important as a common utility, those very devices—if configured and operating properly—are as important to the fulfillment of those flowery mission statements as employees being able to transport themselves to their places of work, the business having reliable power for all of the necessary office equipment (not just the networking gear), and workers being able to communicate via a variety of telephony services.

You ought to be willing to establish a working relationship between a business mission and the networking equipment or solutions. Take a moment to do the following:

- Clearly articulate how the existing network infrastructure and solutions support or detract from the fulfillment of the mission.
- Consider the impact on the business mission if the network or any specific solutions suddenly disappeared and were not going to be available for varying periods of time.

This exercise affords you and all of the stakeholders a bird's eye view of how a new solution is likely to support the mission. And having that bird's eye view provides a necessary refocus during the design stage, when it is easy to lose sight of the ultimate purpose of the design because of the extreme amount of technical detail that must be considered during the design process.

The Pitfalls of the One-Size-Fits-All Approach

Up to this point, the commonality of different SMB types has been stressed in the context of designing a computer network or a networking solution. But even if a network is perceived as a common utility, it is quite obvious that to function properly, the utility delivery systems need to have a proper hierarchical structure to provide effective service—for example, a city water main and high-voltage transmission lines do not terminate at people's homes or at small office buildings. In networking, the logical layers (access, distribution, and core) as well as the level of equipment performance approximate the hierarchies of the common utilities.

The one-size-fits-all approach might attempt to use similar equipment at all network layers and not recognize the need for varying levels of performance of the solutions discussed throughout this book. At one extreme, the pitfall of the one-size-fits-all design approach is overdesign, making the SMB pay for a level of performance or capacity that is much higher than it needs and that is out of range for the business model. This strategy might be adopted so the SMB can use the same equipment models throughout the enterprise. If the SMB makes a conscious decision that the lower support costs resulting from that approach offset the higher equipment costs, there is nothing wrong with this approach. However, this consideration should appear in the design document.

The other extreme of the one-size-fits-all approach is not having sufficient capacity or level of performance at the core or distribution layers. This happens for exactly the same reason as overdesign: The SMB is trying to use the same equipment models throughout the enterprise to save on support and/or configuration costs. Thus, when considering the deployment of either an isolated or an end-to-end networking solution, it is critical to distinguish between the common functions of solutions that span the business sectors, sizes, and missions and the elements of solutions that need to be customized, mostly in terms of equipment models and levels of performance. Common solution functions include the following:

- The generic ability to move information between locations (routing and switching)
- Providing security in terms of confidentiality, information integrity, or prevention of the denial of service
- The ability to support and to integrate with applications

Within each of the preceding common functions, the solution differentiators that must be observed across the spectrum of SMB types and sizes to avoid the one-size-fits-all pitfalls are as follows:

- The level of performance of routers and switches

- The degree of security or the use of integrated versus single-purpose security devices
- The configuration customization that is required to support specific applications

SMB Networking Solutions Design Considerations

The basis of any business transaction is the exchange of perceived value between the transacting parties. Designing a networking solution is not only a technical issue, it is a business proposition and a transaction.

For example, the value of a solution might be found in its sheer novelty, thus creating a perception on the part of an SMB's stakeholders of a business that is innovative, creative, and on the cutting edge of technology. That perception in turn could lead to higher levels of investment or an increase in the customer base that further expands the business. A single converged IP network transcending geographical boundaries and supporting multimedia communications (voice, streaming audio and video, selective video conferencing, and all of the traditional database and resource sharing functions) can be viewed as a trendsetter in ultimate productivity. That kind of perceived value tends to come from early adapters whose business mission (whether formally stated or not) demands that they be perceived as innovative and progressive. The value of a networking solution can also be associated with something that is perceived as a bit more mundane and mainstream, such as an incremental increase in productivity by occasionally allowing an employee to work remotely.

Whatever the SMB's position regarding a networking solution, the value proposition of the solution needs to be clearly articulated because it drives the design process. When considering the design of the solutions in the sections that follow, ponder the fundamental issue of value to the SMB resulting from each solution.

In addition, keep in mind that many solutions are organically grown together. Remote access can be designed for internal employees only, as a part of collaboration with partners, or as a part of customer care. In all instances, it is tied closely to security. Front office/back office integration requires that a solid networking infrastructure already be in place and that the software applications to be integrated are already functioning well.

When designing a networking solution, it is quite easy to be drawn into the process of solving all of the existing network problems that, from your perspective, represent separate issues. However, keep in mind that when it comes to the network, your perception typically has a higher granularity than the view of the executives who have to sign off on the design document and sign the purchase orders for labor and equipment to proceed with deployment. The executives tend to take a more integrated view of the network, in which many issues boil down to a simple question: Will it function well and support the business's goals?

You must always give consideration to the reconciliation of the highly granular versus the highly integrated views of the network. Otherwise, the potential for failure of the design process is high. The executive stakeholders will not sign off on a design that does not give significant consideration to implementation issues.

Network and Data Security Design Considerations

Ponder these questions in the context of considering the deployment of a security solution:

- Has the SMB placed a monetary value on having its computer network inaccessible for varying periods of time, from a few minutes to hours, or even days?
- Is the impact of system unavailability linear as a function of time, or does the impact spiral out of control at a certain point, causing the business to fail or lose a significant market share to competition?
- What is the impact of having employees spend many hours unproductively due to downtime?
- What is the impact of having confidential and proprietary information fall into the wrong hands?
- What is the impact of having mission-critical information imperceptibly altered or outright corrupted?

A key concept to keep in mind while designing security solutions is that a security solution is not equivalent to a security policy. A security solution supports a security policy but is not a substitute for one; that distinction, although it might seem clear, tends to get blurred during the design process if an SMB does not have a clearly defined policy.

SMBs without sufficient resources to afford internal network security staff probably lack a security policy and might be looking to you as a resource for developing it without even necessarily identifying the process in those terms. When you realize that this is happening, you must differentiate between the changing responsibilities: designing a solution to support a policy versus developing a policy that in turn will require one or more solutions to implement it. Although both tasks are valid, developing a security policy might have different legal ramifications than designing a security solution to implement it.

Design considerations for specific security solutions dealing with specific threats and deployment scenarios are discussed in Chapter 5. Chapter 4, "Overview of the Network Security Issues," provides an overview of security issues, including terminology, security threat categories and their respective antidotes, and the importance of developing a security policy before proceeding with any security implementations.

Remote Access Design Considerations

You should consider the following questions before defining the requirements for any form of a remote access solution:

- What is the value of having access to a corporate database anytime and from anywhere?
- Are there any other resources on the corporate network—such as high-performance printers, network management stations, or even individual networking devices—that it would be useful to access remotely?

- Who are the most likely candidates within the SMB's corporate structure to have remote access?
- Who are the least likely candidates for having remote access? Why?
- Is it possible that a mindset has developed that needs to be reevaluated regarding who should and should not have remote access?
- If remote access is offered, what are the acceptable performance criteria for it to be effective?
- What security considerations will accompany any form of remote access?

Answers to those questions drive the design process and determine the specificity of the solution, the remote user categories, the granularity in access levels for different groups of users, and the performance and security criteria for a solution to be effective.

Wireless Design Considerations

What is the value of retaining a connection to the network while maintaining physical mobility? Perhaps mobility in a certain SMB means occasionally carrying a notebook computer from an office cubicle to a conference room and then connecting the notebook to the network in the conference room via a wired outlet in the same manner as it is done in the cubicle. In this case, there probably is not much reason to consider the design of a wireless network.

But what if the work atmosphere at the SMB location is much more dynamic, prewired meeting facilities more limited, and coworkers routinely need to get together to collaborate or to do research on various projects while retaining network access? If a meeting facility has a limited number of wired network connections, it means that a switch might have to be set up locally to provide network access, and cables might snake all over the room—not exactly a scalable or productive environment. What is the value of a wireless solution under those circumstances? Also, consider an automated production facility in which requests for inventory delivery from a manufacturing floor must be transmitted to mobile operators on the warehouse floor. The need for a wireless design in this situation would be greater than in a business that requires only an occasional walk from a cubicle to a conference room.

You need to consider the following questions, and possibly others, when designing a wireless solution:

- Are productivity gains (due to mobility while retaining network access) or savings (from not having to install cabling and cross-connect closets) sufficiently offsetting the cost of design, installation, and maintenance of a wireless solution?
- How secure will the solution have to be, and where will the access points need to be located, to provide sufficient coverage for those authorized to use the wireless local-area network (WLAN) and yet not let it extend beyond the facility to public areas where anyone can tap into it?
- Is the wireless approach considered only for LANs or for WANs as well?

- Will the SMB proceed with a radio frequency (RF) site survey, which is always strongly recommended for larger wireless installation, or will a site survey be skipped, with all of the attendant implications of not identifying potential sources of interference, connection boundaries, and RF dead spots?

The Cisco wireless solution is discussed in Chapter 6, "The Wireless LAN Solution."

IP Telephony Design Considerations

What is the value of deploying an IP Telephony solution if the existing telephone system already works well? You can assume that an SMB will have some form of a telephony infrastructure already in place. There are plenty of questions to ask when considering an IP Telephony solution:

- What is the investment (in terms of time and money) that has been put into the existing infrastructure? Does the high-level design approach require leaving what is already in place (and not changing it in any way), replacing it entirely, replacing it partially, or integrating it with new equipment?
- How old is the existing telephony infrastructure?
- What is its level of depreciation?
- What are the recurring maintenance costs?
- What is the level of expertise required on the part of support personnel for moves, adds, and changes to the infrastructure, and how long does it take to accomplish them?
- How are phone calls made within the enterprise?
- How are phone calls made outside of the enterprise?
- Is the enterprise a single building, or does it encompass multiple locations?
- Are the calls between the locations toll or local calls?
- Is a private data network between the locations already in place? If so, what is the capacity of that network?
- Is the network perhaps already multiplexing traditional Public Switched Telephone Network (PSTN) lines with data?
- Does the SMB have a sufficient number of lines for outside calls, or do employees run into problems when attempting to dial out?
- Does the SMB know if the customers calling in get a lot of busy signals because of an insufficient number of lines, or is it easy to get through?
- What are the features of the current system that are most frequently used? Are there features that nobody uses? If so, why? Is it because they are too difficult or cumbersome to use, or are they simply unnecessary?
- Is there a list of features that users deem desirable that are not available within the current system?

Telephone service is considered a common utility, and overhauling any kind of utility represents an overhaul of an element of the business infrastructure, which can have a significant impact on business operations. When considering IP Telephony, the issue of Voice over IP (VoIP) inevitably comes up. Although IP Telephony is closely coupled with VoIP, to the point where the two expressions are often used interchangeably, there is a difference between them.

VoIP is the enabler for IP Telephony. VoIP represents a technology that encompasses numerous protocols and standards from the Internet Engineering Task Force (IETF) groups and from the International Telecommunications Union Telecommunications Standardization Sector (ITU-T) to allow the transmission of voice traffic over a packet-switched (IP-based) as opposed to a circuit-switched network. IP Telephony refers to the utilization of VoIP to create telephony systems with many advanced features that are not available in traditional circuit-switched telephony installations.

In the context of more than a century of telephony history, VoIP is a relatively recent phenomenon—it is a newcomer that dates to the mid-1990s. However, since its inception, there has been a general consensus in the industry that VoIP has progressed through at least three generations and that its impact has been felt widely in both the carrier and the enterprise markets through ever-more-sophisticated IP Telephony solutions, which are discussed in Chapter 8.

Partner Collaboration Design Considerations

The following questions are just some of the queries that you will need to address to develop a direction for deploying a collaboration solution:

- What is the business value of collaboration with partners?
- What exactly is the manner of the collaboration that an SMB envisions? Is it a matter of one of the following?
  - Providing partners with remote access to internal proprietary tools or knowledge databases on the SMB's network to facilitate problem solving related to the SMB's products that the partners support
  - Having a team of individuals drawn from a group of partners being able to work together effectively for a short period of time on a marketing or an engineering project
  - Setting up an e-mail list to enable the required collaboration
- Is the use of e-mail without even setting up a special list adequate?
- Does the collaboration require exchange of design documents that are subject to strict version control?

Usually, a collaboration solution with business partners, vendors, or even customers boils down to providing them with appropriate access to some of the SMB's internal resources.

That, in turn, can ease the pressure on the SMB's personnel to interact with the relevant parties over the phone, via e-mail, or in person.

The key issues to consider when granting access are as follows:

- What is the level of access to be granted to the partners?
- Does the resulting increase in the SMB's operational efficiency and the savings in personnel time sufficiently offset the resources required to set up the appropriate access levels and to offer the necessary training and technical support to ensure that the setup is being used effectively?

By definition, providing varied access levels from the outside to internal resources implies having to consider the issue of security, which in turn implies a security solution. And the implementation of a security solution should be subject to a security policy. The process of developing a security policy is discussed in Chapter 4.

The mechanics of enabling collaboration with partners, vendors, or customers could require setting up a server on one of the SMB's demilitarized zones (DMZs) or providing virtual private network (VPN) access to the SMB's internal servers residing on the private network. It is entirely possible that SMB's personnel might already have a VPN set up to access the internal network. If VPN access is offered to partners, it becomes a matter of configuring proper authentication, restricting authorization to the relevant resources, and periodically generating reports about their activities. Setting up access to a DMZ server could also take place via a VPN. Alternatively, it could be set up in a more open way, where everyone has access to that server but must log in with a password. More open access to the server on the DMZ could result in greater reliance on the server's operating system (OS) security features to protect it from being breached, which implies that the OS's security level would have to be consistent with the SMB's security policy.

Customer Care Design Considerations

What is the value of an effective customer care solution? It is the lifeblood of a business! Any self-respecting business is well aware that without properly caring for its customers and offering them value for its products and services, it is not likely to stay in business for too long. But what exactly is a customer care solution? Customer care solutions vary as a function of business size and sector.

However unique or standard a customer care solution turns out to be, it is generally enabled via the networking infrastructure. The solution could be as simple as having a well maintained website with routine updates about a company's products or services. The website could be further enhanced with online ordering capability and spruced up with regularly updated links to URLs deemed of interest to the customer base. Customer care might mean regular communication with select customers via e-mail about special offers. Or it could require an IP-enabled call center offering 24×7 technical or problem-resolution support. It could also call for access to internal resources as a function of the customers'

relationship with the SMB. Those resources could be digital documentation, technical information relating to the purchased products, or downloads of software updates or bug fixes if the SMB is a software vendor.

Just remember that a key design consideration for any customer care solution is its ongoing availability after it is released to the customer base. If a customer care solution is offered but it is unreliable because it does not work well or it is routinely unavailable, the situation can lead to a high degree of frustration on the part of the customers and can ultimately defeat the very purpose for which the solution was developed.

Front Office/Back Office Integration

Perhaps you are wondering what front office/back office integration has to do with networking solutions to begin with. It is simple—think applications. As mentioned earlier in this chapter, the network routing/switching infrastructure, as well as any of the other networking solutions (security, remote access, or wireless), must support and integrate well with the existing or planned applications.

The applications that customers "interact" with directly that relate to sales and marketing are customarily referred to as *front office* (facing the customer) *applications*. Those applications could include order entry, customer profiles, or general account maintenance in a call center or via a self-service, web-based interface. The applications that support the processes that are not directly seen by the customer (order processing, production, inventory control, or other accounting functions) are typically considered the *back office applications*. The back office applications are also referred to as the enterprise resource planning (ERP) applications.

What is the value of having the front and back office applications integrated into an effective customer relationship management (CRM) system? That is the question that the SMB's executive stakeholders need to answer. Making that decision will probably be a far more complex process than deciding to deploy network security or remote access. However, if the SMB decides to proceed with a custom, in-house integration or an off-the-shelf CRM solution, it must ensure proper connectivity between the relevant locations and sufficient bandwidth and processing power within the networking infrastructure to allow for the exchange of data generated by the CRM solution. Although it might not be absolutely critical for you to understand the specific functions of each of the applications, it is critical to understand the load that they place on the network and their security features.

The integration process might also require a specific functionality, like the support for multicasting within routers and switches or the addition of wireless LAN because a portion of the CRM is useless without the wireless mobility. From a security perspective, with integrated applications, the level of granularity in access and authorization becomes far more critical than with standalone isolated application islands.

Solution Identification and Discovery Process for SMBs

It is hard to imagine that today a successful SMB of any size is going to function without a networking solution, even if it means the most rudimentary file or printer sharing. When prioritizing the spectrum of networking solutions according to their importance and deployment, it is helpful to categorize them in terms of direct versus indirect support of the business mission.

If a wireless solution is a must in a manufacturing facility because of the impracticality of running cables or the exorbitant costs associated with doing so, that wireless solution directly supports the business mission. Forms of remote access in this scenario might be deemed desirable but not necessarily critical to the direct support of the business mission. Security considerations apply to both wireless and remote access deployments. Thus, in this example, the identification process yields that a wireless solution is a must, relevant security in support of it is a must, overall security is a distant second, and remote access is a "nice to have" capability that might happen someday. Following are some of the con and pro arguments for deploying various solutions.

The Case Against and for a Security Solution

The obvious case against a security solution (as well as any other networking solution, for that matter) is that the solution is complex, partial at best, and expensive to implement and to maintain. As discussed in Chapter 5, Cisco security solutions run the gamut in terms of ease of implementation, range of threats that they protect against, and cost.

What any SMB contemplating a security solution ought to know is that a security vendor like Cisco is not in the business of developing specific security policies for SMBs. In the process of attempting to sell a solution, a vendor can offer assistance in guiding the development of a security policy, but the SMB must recognize that without a policy and without the business placing a value on the assets to be protected, it is easy for the SMB to shoot down any proposed solution. So the SMB must clearly communicate to the designer the need for a solution and the degree of required protection before arguing against the solution because of its cost or complexity.

If an SMB has nothing to protect, the case against a security solution is clear-cut: There is no need for one. If an SMB comes to the conclusion that its network and information assets are worth protecting, the case for a security solution is even more clear-cut: It should get one. If the SMB reaches this conclusion, you can begin to determine the appropriate solution from a range of choices.

As discussed in Chapters 4 and 5, implementing a security solution is not a static, one-time event; it is an ongoing process of reexamining the value of what needs to be protected

against the well-known and emerging threats to determine if the degree of deployed protection is adequate. The good news is that, as a general rule, security solutions from Cisco are getting easier to deploy, offer an increasingly comprehensive and integrated level of protection against varied threats, and are geared toward a spectrum of SMB budgets.

The Case Against and for a Remote Access Solution

The case against a remote access solution might be as simple as the perception on the part of an SMB that a solution is not needed because the business does not understand the possibilities associated with it. In that case, you should make sure the SMB considers the business possibilities that a remote access solution offers.

Remote access by itself is a generic solution without a face. But what if it translates into the following?

- A flexible work environment, by allowing employees occasionally to work from home, thus boosting employee morale and commitment to the business
- A high degree of collaboration with business partners, thus decreasing time-to-market cycles and boosting productivity
- Improved customer service, by allowing customers to place orders online, view order status, or search through an SMB's databases

These benefits sound like e-commerce, customer care, or just online access, but underneath them is the ability to remotely access SMB's resources. Every time someone logs on to the Internet, it is a form of remote access. Try taking that away from businesses and individuals alike and observe the impact.

The case for a remote access solution is quite compelling if the prospective SMB considers the solution in terms of business activities that it facilitates and the resulting value that it creates for the business. Remote access is the ultimate enabler of modern-day business communications. Strong security that is currently available through VPNs and firewalls adds to the appeal of remote access solutions.

The Case Against and for a Collaboration with Partners Solution

Making the case against or for a collaboration with partners solution depends to a large extent on the existing SMB's network implementation. For example, if an SMB already has an effective VPN solution, then granting outsiders access to internal resources becomes a matter of Authentication, Authorization, and Accounting (AAA). Separate Virtual LANs (VLANs) for different partners on the SMB's internal network might be the result of

applying the AAA principle to partner access. If an SMB already has a firewall solution with one or more DMZs, collaboration with partners might also be a matter of providing them with the needed resources on the DMZ networks.

Because any collaboration solution is closely tied to security, an SMB should have a well-developed security policy and update it when a collaboration solution is being considered.

If remote access and, consequently, security solutions are not in place, there might be a stronger case against collaboration with partners because that solution might require a more comprehensive design. It depends on how exactly collaboration with partners is defined. Simple collaboration could be a matter of additional configuration or setup without any new hardware or software. However, remote access and security already in place will ease any collaboration deployment and create a strong case for it, subject of course to SMB's business objectives. Naturally, not every SMB is going to have partners to collaborate with.

The Case Against and for a Customer Care Solution

There is really no effective case against a customer care solution. No magic formula defines such a solution because it is unique to each business, but if this lack of a clear-cut definition is used as an argument against designing and implementing one, it is a weak argument at best.

The case for a customer care solution is simple. Other networking solutions—including IP Telephony, security, wireless, and the well-developed networking infrastructure—all stand in support of developing effective customer care, whether it takes the form of a call center, online banking, or VPN access by customers to internal resources.

The Case Against and for a Front Office/Back Office Integration Solution

The overwhelming case against a front office/back office integration solution is that it is generally a complex process that requires a lot of up-front planning and preparation. Such a process is not something that a typical SMB might be readily willing to undertake given the high level of risk associated with the entire process, the level of project management expertise required to see it through to completion, and the required degree of understanding of the existing applications environment and business processes.

The case for a front office/back office integration solution is equally strong. It can increase revenues and reduce costs through more focused and targeted customer service and the reduction of production overhead or the cost of sales. The availability of high-performance computing platforms and networking infrastructure that is capable of large throughput over long distances facilitates the deployment of complex applications, which an integrated CRM/ERP application suite can certainly be.

Summary

Designing a networking solution with the intent of bringing it to fruition through implementation is a business transaction. It is in your and the design process's best interest if that transaction is perceived by an SMB as valuable.

Business sizes and sectors usually impact the quantity and the level of equipment performance within a networking solution. As a general rule, all SMBs share the need for similar solution functions. Modularizing the enterprise and adhering to hierarchical interconnection of the infrastructure components (routers and switches) become keys to a scalable network design.

Cisco offers a spectrum of products in each solution category to accommodate varying business sizes. Any networking solution must support applications that are unique to varying SMB categories and critical to any SMB's success. Networking solutions do not operate in isolation; there is interdependency between them, with certain solutions being the enablers for others. Each networking solution has pros and cons that should be considered before proceeding with design and implementation.