# Deploying the All-IP SMB Office


## Abstract

In today's competitive business environment, companies of all sizes are relying on network-based applications and communications tools more than ever before. As small organizations look to improve employee productivity, cut costs, expand services, and accomplish more with less, the advantages of Internet Protocol (IP) technologies, and of maintaining an all-IP network, are becoming more and more compelling. Deploying and maintaining a modern IP network, however, can be a complex and time-consuming proposition. The challenges can be particularly difficult for smaller organizations with limited technology budgets and limited in-house IT expertise.

This paper discusses the advantages of IP network technologies for small businesses and details many of the factors that companies should consider when deploying an all-IP network. The paper also introduces the broad range of Cisco® IP solutions that have been designed specifically for smaller organizations. These technologies deliver all of the benefits of IP technology in a simple, affordable, and easy-to-deploy solution.


## Harnessing the Power of the IP Office

The rise of the Internet and modern business technologies has leveled the economic playing field, allowing companies of all sizes from all parts of the world to compete for customers and dollars. This connected global marketplace, however, also means more competition, especially for small businesses. More than ever before, small companies are looking for ways to reduce costs, improve employee productivity and efficiency, and enhance customer service and loyalty. Small companies also need ways to take advantage of new Internet-enabled tools and markets without leaving their assets, customer data, and good reputations vulnerable to network security threats.

For many organizations, the solution to addressing all of these objectives lies in migrating to an all-IP office. When all technologies in the office are based on a common technology (the Internet Protocol data standard), you can create an environment in which all people, processes, systems, and technologies in the office are linked within a single, secure, and intelligent network. This pervasive interconnectedness makes people and processes more flexible and responsive, and allows your business to operate more efficiently and profitably.

The primary benefits of maintaining an all-IP office include:

- **Convergence**: An IP office connects all of your business resources, employees, customers, and suppliers in a single, secure network. It integrates previously separate systems and processes within a single environment and allows you to deliver data, voice, and even video over a single IP network. When all devices and systems in the office support IP, all of the resources in the office—PCs, servers, telephones, wireless access points, fax machines, copiers, video surveillance cameras, and so on—become intelligent, interconnected endpoints in a single network. A converged IP network also allows you to explore the advantages of "in-person" communications with customers, employees, and partners anywhere in the world through videoconferencing. In an IP network, voice, video, and data communications are all just different types of IP traffic.

- **Reduced costs**: Instead of operating voice, data, and video services as distinct networks, you can save money by collapsing these multiple networks (as well as the processes required to support them) into a single system. For example, by providing telephone services over the IP network (referred to as unified communications, or IP telephony), you can make it much easier and less expensive to handle phone moves, adds, and changes. Instead of having to wait weeks for the phone company to install a new internal line, you can add an extension yourself in minutes and just plug in the new phone. If your business has multiple locations, you can eliminate long distance charges for site-to-site calls by carrying them over the data network (referred to as voice over IP, or VoIP).
- **Increased employee efficiency and productivity**: After your business has moved from paper-based processes to IP, employees can collaborate and communicate more easily and access the resources they need wherever they need them, even remotely. With solutions such as unified communications (applications that take advantage of converged voice, data, and video services), you can move communications across multiple systems and devices to improve employee connectedness and responsiveness. Employees can access voicemails, e-mails, and faxes from a single inbox and retrieve messages in whatever format is most convenient at the time (for example, “listening to” e-mails from a cell phone on the way to work). With intelligent IP call routing, any IP phone in the office, or even at the employee’s home, can become an “internal” business extension. Employees simply log on to the phone, and the office network dynamically routes all calls where they need to go.
- **Improved business resilience**: IP makes it possible to separate your essential business applications from the physical hardware on which they operate to help ensure nonstop operation. For example, you can run a single application on two virtual servers, one of which might be located remotely. A flexible IP network also allows you to use powerful data backup and disaster recovery tools to easily back up your essential business data on remote servers, instead of onsite file cabinets, to help ensure that your business can continue to operate even after a catastrophic event.
- **Increased scalability and flexibility**: An all-IP network makes it easier to add applications and capabilities over time. Whether you are considering new customer service applications, supply chain applications, or other business productivity tools, as long as it is an IP application, the entire network can support it. Alternatively, if you invest in a proprietary technology solution, it might be out of date in just a few years. When you implement an IP foundation, you can continually evolve your network with your business.

Large companies have enjoyed the advantages of a unified, all-IP network for years. Now, a new class of simple, affordable IP solutions is making these benefits available to small organizations. However, to implement these solutions successfully, you need to make sure that the IP network you deploy meets core requirements for performance, security, manageability, and simplicity.

### Considerations for Deploying the All-IP Office

An all-IP office encompasses a variety of basic network, security, voice, and wireless technologies, including:

- The wide-area network (WAN)
- The local-area network (LAN)
- Unified communications technologies

- Security systems
- Wireless networking solutions
- Network management tools
- Network support services

Before any of these solutions can begin having an effect on your business operations, however, you need to make sure that your network meets fundamental requirements for bandwidth, quality of service (QoS), security, availability, and manageability. For you to realize the benefits of an all-IP office, these baseline capabilities must extend across all segments of the network.

**Bandwidth**

How much bandwidth is enough? The answer is different for different companies. In order to get the most from your IP network, your Internet connection as well as your router and all of your switches should provide enough bandwidth to support the applications (data, voice, video) you plan to run on your network.

To protect your investment and preserve the longevity of your IP network, you should build the network with more capacity than you currently require. For example, the basic applications you use today might work well with 10-Mb-per-second (Mbps) LAN switches and wireless access points. However, if you deploy 10-Mbps technologies today and then later decide to deploy an application that requires higher data speeds (such as IP video), you will have to replace that LAN infrastructure.

When considering your WAN or Internet connection, in contrast, you do not need to pay for additional bandwidth that you will not use, as long as the connection can support your needs for the present and the immediate future. As you prepare to roll out an all-IP office, it is a good idea to talk with your Internet service provider or WAN provider about your plans and ask that provider to evaluate your likely bandwidth needs to help ensure those needs are met.

**Quality of Service**

A delay of a fraction of a second is unnoticeable for an application like e-mail, but that same delay can make a phone conversation impossible. For productivity-enhancing applications like IP telephony to deliver their full value, your IP network must employ QoS intelligence to prioritize delay-sensitive voice and video traffic.

The benefits of QoS capabilities, however, extend beyond IP communications. To preserve the performance of your essential business applications, the network also should be able to identify and restrict other nonessential types of network traffic when necessary. For example, the network should recognize abnormal traffic patterns that result from a network attack such as a distributed-denial-of-service attack and be able to restrict that traffic before it can overwhelm your business applications. An IP network can even employ QoS intelligence to control nonmalicious yet potentially disruptive traffic such as YouTube video streaming or peer-to-peer file-sharing services that employees might be using recreationally. Without the ability to recognize such traffic and either block it or limit the resources devoted to it, this recreational network activity can quickly impede your business applications.

In all cases, you should make sure that your network supports QoS end to end. This is especially important if you are using IP voice or video applications. If just one network component does not

support the traffic prioritization that these applications require, it can negatively affect the entire network.

### Security

In the past, security for many small companies meant simply deploying a firewall. Today, as network threats have increased in number and sophistication, you need much more robust, pervasive protection. You should also recognize that most security threats originate from inside the firewall, either from an attack that has infiltrated your internal network and launched there or from an employee's own actions, whether malicious or unintentional. Today, protecting your internal LAN is just as important as protecting your WAN connection to the outside world.

The Cisco model for network security encompasses four primary areas to consider when building an all-IP office:

- Threat detection and prevention
- Secure connectivity
- Data theft prevention
- Trust and identity services

Of course, this model addresses only your network security. You should also make sure you have the appropriate physical security systems in place to protect your business premises and equipment.

### Threat Detection and Prevention

Computer worm and virus attacks remain the most common security threat to small businesses. A successful attack can wreak havoc on business servers and employee PCs, impeding productivity and potentially shutting down important business processes for hours or days. To protect your business and your customers, your network must be able to quickly identify viruses and other network attacks and dynamically prevent them from disrupting or disabling your business applications. To do this, your network should include:

- **Firewall capabilities**: Firewalls inspect all incoming traffic at your network perimeter (your connection to the Internet or the WAN) to help ensure that only legitimate traffic can enter the internal network. These capabilities can be provided by a standalone firewall appliance or by software features built into your network router.
- **Intrusion detection system (IDS)/intrusion prevention system (IPS) capabilities**: Because network attacks have become more sophisticated, your network needs the intelligence to continually recognize and react to evolving threats. IDS/IPS technologies quickly identify and block any suspicious or threatening behavior on the network. As with firewall capabilities, you can deploy these services using a standalone network security appliance or through software features on your network router. If your business uses many Web servers or employs many mobile workers with laptops, you might also want to consider host-based intrusion detection software that resides on servers and PCs to monitor operating systems for any suspicious behavior.

### Secure Connectivity

One of the best ways to increase employee productivity and responsiveness is to provide remote connectivity options that allow employees to access business applications and e-mail while away from the office, over the Internet. Today's employees can find Internet access virtually anywhere

and work productively from an airport, hotel, café, or even home. However, to support remote workers, you need to make sure that employees can connect with business resources securely over public networks.

Virtual private network (VPN) capabilities provide strong encryption that allows external users or systems to connect with your business network over the Internet using secure, private channels. Both your site-to-site WAN connections and the connections your employees use to log into the network from remote locations should employ VPN technology. You can use a standalone VPN appliance to provide remote connectivity, but you might prefer to have the option of managing VPN connections using software on your network router.

**Data Theft Prevention**

With more and more people transmitting their personal and financial information online, information theft has become extremely lucrative and, as a result, increasingly common. Often, cybercriminals view small businesses as ideal targets, because they tend to be less protected than large enterprises. For small businesses, a successful breach of protected customer data can be extremely damaging, leading to loss of customer trust, diminished reputation, and, potentially, costly legal action.

To safeguard your business, you need network security that can protect against “man-in-the-middle” attacks. These attacks are insidious because they allow thieves to intercept data traversing your network without leaving a trace, leaving you exposed and unaware. Your network should feature state-of-the-art security features that help ensure that sensitive information is only transmitted over secure channels and that block common man-in-the-middle attack strategies.

**Trust and Identity Services**

You need to be able to tightly control who can access your network. Most likely, you will need different levels of control for internal staff, as well as for external partners and suppliers who might require access to some segments of your network. Your network infrastructure (routers, switches, wireless access points, etc.) should be able to control and block access to the network. Your network also should provide tools to tightly control how information is exchanged among different applications and processes, and to help ensure that private information is not accessible from public-facing segments of your network.

You may also want to look for network devices that support advanced access control services. For example, network switches that support 802.1x identity-based networking services can help ensure that only authorized users and applications can access your wired and wireless LAN. Network Admission Control (NAC) services verify that any user or device attempting to access the network meets baseline security requirements (such as having up-to-date antivirus software) and blocks access to those that do not. Even if you do not plan to deploy advanced security services immediately, you should consider network technologies that will allow you to quickly implement these services in the future as your business and its security profile grow.

**High Availability**

Even the most advanced, powerful IP applications are of no use if the services they provide are not continually online and accessible to your employees and customers. So you need to evaluate the resiliency of your applications and your business at every point in the process of building your IP network.

Perhaps the most important aspect of business resiliency is continually backing up your essential business data. As many companies learned the hard way in the wake of floods, hurricanes, or other catastrophes, it is not enough to back up data to a secondary data store on the premises. Your IP office should include a data backup/disaster recovery strategy that allows you to easily and continually back up data to a remote location.

Your network also should support onboard diagnostics and monitoring to alert you to potential issues before they impact your business. For many companies, the best solution is to work with an IT partner who can monitor your business network at all times and address any issues that arise.

You should also build redundancy into your network: for example, installing a backup router that is configured to come online if the primary router fails to help ensure that an issue with one device or application cannot bring down the entire network. Many companies extend redundancy to power supplies as well to protect against power failures. When choosing network hardware, you should make sure you are using business-class equipment built by a proven vendor with a trusted design and manufacturing process. While the consumer-grade equipment available at retailers might be fine for a home network, such equipment rarely provides the resiliency and feature set required in a business environment.

#### Manageability

The ideal small-business IP network should not be a complex, unwieldy environment that requires advanced network engineering skills to support. You should be able to quickly deploy and easily control the entire end-to-end infrastructure, even without a full-time network expert on staff. To help ensure simplicity, you should make sure that all of the network components you are deploying—including data, voice, video, and wireless solutions across the entire network—can be controlled and configured from a single, easy-to-use management interface.

### Components of the IP Office Network

Your IP office network might consist of WAN and LAN devices, IP communications technologies, wireless access points, and network management tools, as well as services to support and protect your network. Each segment of the network has its own unique requirements and considerations. Fortunately, Cisco provides affordable, easy-to-deploy small-business solutions across all segments of the network that are designed to fully integrate and function as a single system.

#### The Wide-Area Network

The WAN connection is your link to the outside world, including your customers and partners, as well as any remote business locations. When it comes to voice and data services today, many smaller businesses rely on a voice trunk from the phone company (usually a fractional T1 line) to connect internal office phones to the public telephone network. For the internal extensions within the office, small companies typically use a traditional phone switching system, such as a small-scale private branch exchange (PBX) or key system. For data and Internet services, many small to medium-sized companies use T1 Internet connections, while smaller companies often use a cable or digital subscriber line (DSL) broadband connection. When choosing the voice and Internet connection for your office, you should carefully consider the types of applications you plan to run on your network today and in the immediate future. While traditional small-office voice and data connectivity can meet basic needs, it does not allow businesses to fully integrate voice and data services and limits the types of applications they can deploy.

From a technology standpoint, the cornerstone of your WAN connection is your network router, which links your LAN to the Internet or to the private network connecting your sites. If you are using IP telephony or VoIP solutions, you will need a voice-capable IP router that can act as the gateway between your office network and the public telephone network and that can convert conventional voice traffic to IP, and vice versa. If you have multiple sites, you will also want to work with a WAN provider that can deliver the QoS necessary to carry your site-to-site calls over the data network to eliminate long-distance toll charges.

In order to provide strong security for your business while keeping your network costs and complexity low, you should choose a router that provides built-in security and VPN features. Routers with software-based firewalls, IPS/IDS capabilities, and VPN capabilities eliminate the need to deploy separate devices for these functions. For simplicity's sake, you also might want to consider an office router that provides built-in support for wireless networking. If you operate out of a small office, one wireless access point might be sufficient to support the entire site. In this case, you might want to consider a router with an integrated wireless access point.

WAN solutions to consider include:

- **Cisco 800 Series Routers**: The Cisco 800 Series provides the ideal access router for small businesses using basic broadband Internet connections. The solution includes four 10/100-Mbps Ethernet switch ports, integrated firewall and VPN capabilities, QoS features to support voice connectivity, and native support for 802.11b and 802.11g wireless LANs.
- **Cisco 1800 Series Integrated Services Routers**: The award-winning Cisco 1800 Series was designed specifically to provide small and medium-size businesses with everything they need to connect a small office in a single solution. The Cisco 1800 Series offers full voice and QoS capabilities and integrated 82.11a/b/g wireless support. Robust security features include integrated firewall, IPS, and NAC services, URL filtering to control the which Websites are accessible from the business LAN, and support for as many as 50 VPN connections. The solution also features eight 10/100-Mbps Ethernet switch ports with optional Power over Ethernet (PoE) capabilities that allow you to power network devices such as IP phones and wireless access points over the Ethernet connection.

**The Local-Area Network**

The LAN equipment is the backbone of the all-IP office. Every business LAN is unique, depending on the size of the business, the number of employees and users, and the types of applications the LAN supports. To build a scalable, high-performing LAN backbone, you should be sure to address the following considerations:

- **Switch ports**: All of the PCs, wireless access points, IP phones, and other wired network devices in the office connect with the LAN by plugging into a port on a network switch. When choosing switches for your network, make sure you have enough ports to support all of your IP devices, as well as excess capacity to allow you to grow your business without having to invest in new infrastructure equipment. You should also make sure that your switches deliver the data speeds necessary to support your needs. For most small business applications, 10/100-Mbps Ethernet is more than adequate. Businesses that share very large files over the network or use high-bandwidth media applications might need Gigabit Ethernet capabilities.
- **Power over Ethernet**: PoE-capable switches allow you to power your IP phones, wireless access points, and other IP endpoints directly over the Ethernet cable without requiring a

separate power source. PoE has become a core requirement for many businesses' wireless networks, since wireless access points often are deployed in ceilings where independent power sources might not be available.

- **Quality of service**: Even though different devices might claim to support QoS capabilities, not all QoS is the same. Make sure you have the right QoS for your applications. You might need more than just the ability to identify some types of traffic as high-priority. For example, you might want your network to be able to identify and drop traffic that is not time-sensitive to help ensure that IP voice calls and other mission-critical information traverses the network as quickly as possible. Your LAN devices and management tools also should allow you to easily configure QoS for the entire network.
- **LAN security**: To protect your business and your customers, you cannot afford a vulnerability at any point in your network. In order for your network to operate as a single, secure environment, you need LAN switches that support centralized user authentication and access control services, including NAC if you plan to deploy it. Your LAN switches also should provide integrated port security features, as well as VLAN capabilities that allow you to partition your network so that sensitive data cannot be accessed on publicly accessible segments of the network.

LAN solutions to consider include:

- **Cisco Catalyst® Express 500 Series Switches**: The Cisco Catalyst Express 500 Series offers best-in-class networking for small and medium-size businesses. This family of Layer 2-managed Fast Ethernet and Gigabit Ethernet switches offers exceptional performance and security in a network foundation optimized for data, wireless, and unified communications services. The Cisco Catalyst Express 500 Series also offers QoS and PoE options to help reduce the cost and complexity of deploying IP telephones and wireless networks.
- **Cisco Catalyst Express 520 Series Switches**: The Cisco Catalyst Express 520 Series Switches are components of the Cisco Smart Business Communications System, an integrated system of voice, security, and wireless networking products. These fixed-configuration, managed Fast Ethernet and Gigabit Ethernet switches provide the reliability, scalability, and a rich feature set small and medium sized businesses need in a cost-effective, easy-to-manage platform. These switches provide a secure, high-performance foundation with quality of service and power over Ethernet features to support essential business applications with a single, comprehensive platform.

**Converged Voice and Data Technologies**

In addition to using a voice-capable IP router and network switches that support PoE, you will need an IP call processing solution to provide IP telephony and VoIP capabilities in your office. IP call management platforms interoperate with your IP router and the public telephone network to route phone calls over your IP network. A successful IP voice solution also requires end-to-end QoS in the office LAN and WAN to help ensure consistent call quality. And, of course, you will need IP phones that provide the right mix of features and affordability for your business.

Cisco Unified Communications products to consider include:

- **Cisco Unified Communications Manager Express**: Cisco Unified Communications Manager Express provides a cost-effective and highly reliable unified communications solution for small offices. This platform, embedded in the Cisco IOS® Software that resides

on Cisco integrated services routers, provides all of the call processing capabilities small businesses require to deliver a comprehensive set of services and features up to 240 IP phones. The platform includes advanced call handling capabilities as well as an intuitive management interface for easy installation and phone moves, adds, and changes.

- **Cisco Unity® Express**: Cisco Unity Express provides full voicemail, greeting, and interactive voice response (IVR) capabilities in a single, comprehensive solution designed specifically for small businesses and branch offices. The solution provides rich messaging and greeting services, Web-based administration of voice mail and autoattendant services, the ability to manage messages using an e-mail client or the visual display on an IP phone, and scalability to 250 mailboxes.
- **Cisco Unified Communications 500 Series for Small Businesses**: The Cisco Unified Communications 500 Series provides a simple, affordable, and easy-to-manage unified communications system designed exclusively for small organizations. The solution eliminates the need for multiple servers and devices by combining telephony, messaging, and wireless mobility into a single, simplified device.
- **Cisco Unified IP Phones 7900 Series**: Cisco Unified IP Phones 7900 Series allow you to take full advantage of your converged voice and data network while retaining the convenience and user-friendliness you expect from a business phone. Available in several models to meet different user needs and price points, this family of IP phones features LCD displays and dynamic soft keys to control advanced call features. Cisco IP phones also support the integration of customized business applications and services, for example, allowing employees to access company directories, streaming stock quotes, or other Web-based services using the phone's LCD display.

**Wireless Networking**

Many companies now recognize the productivity and mobility benefits of wireless networks in the office. Without proper planning, however, a substandard wireless implementation can be difficult to manage and leave businesses vulnerable to data theft and other network threats. When planning your wireless deployment, you will need to address four primary concerns:

- **Wireless management**: Wireless networks typically are deployed either as "autonomous" systems (in which the bulk of the data processing and network intelligence is located in each individual access point) or "unified" systems (in which data processing, security, and other intelligence are managed from a centralized wireless controller). A unified system might be a better choice in larger deployments, because it allows you to centrally configure and control all access points in the network instead of having to manually configure each individual access point. In small offices where one or two access points are sufficient, however, autonomous systems might represent a simpler, more affordable solution.
- **Support for IP voice**: If you plan to use unified communications and IP telephony solutions in the office, you should make sure your wireless network can provide the QoS necessary to support voice services. Even if you are only using wired IP communications services at present, voice-capable wireless access points will allow you to quickly and easily add wireless IP phones in the future without having to invest in a new wireless infrastructure.
- **Guest access**: Guest access capabilities allow you to create a Wi-Fi hotspot in your office that customers and visiting partners and vendors can use to connect to the Internet while on your premises. These networks use VLANs to help ensure that public users cannot access your business network or information.

- **Wireless security**: To protect your business and your customers, you need to make sure that your wireless network provides business-class encryption and authentication services. You should also look for wireless solutions that provide features to detect and block “rogue access points” and other common strategies that cybercriminals use to intercept wireless data.

Wireless solutions to consider include:

- **Cisco Mobility Express**: Designed specifically for small and medium-sized businesses, the Cisco Mobility Express Solution cost-effectively delivers business-class mobility features, standards-based security, built-in reliability, and simplified management. The solution, part of the Cisco Smart Business Communications System, provides all of the capabilities you need to easily deploy, manage, and evolve your wireless network.
  - **Cisco 500 Series Wireless Express Access Points**: The Cisco 500 Series Wireless Express Access Point is a single-band 802.11g access point ideal for small businesses with carpeted offices or similar indoor environments. The solution provides enterprise-class security, performance, and flexibility at an affordable price. Easy to deploy and manage, the Cisco 500 Series can be supported in autonomous or controller-based mode to accommodate a wide range of deployment and business mobility requirements.
  - **Cisco 500 Series Wireless Express Mobility Controller**: The Cisco 500 Series Wireless Express Mobility Controller is designed to optimize the wireless networks of small businesses. As a core element of the Cisco Mobility Express Solution, the mobility controller is built to specifically support Cisco 500 Series Wireless Express Access Points. Together, they provide you with complete visibility of the wireless network. The mobility controller automatically manages access points to reduce interference, avoid coverage gaps, and maximize available bandwidth to help ensure optimal overall network performance and supports advanced mobility services such as guest Internet access and voice over Wi-Fi.

**Network Management**

Although many small businesses can envision how a modern IP network could benefit their employees and customers, the prospect of managing all of the devices and applications in the network can seem daunting, especially for small companies with limited IT expertise. Even when a specific IP technology has an easy-to-use management interface, you need to make sure that you can manage that technology as part of a single, integrated system, instead of having to learn multiple interfaces to control each part of your network. Cisco offers several management tools to help small businesses easily configure and control their networks.

- **Cisco Configuration Assistant**
  Cisco Configuration Assistant provides a comprehensive, easy-to-use solution for managing all routers, switches, IP communications solutions, and wireless access points in your Cisco Smart Business Communication System. Cisco Configuration Assistant simplifies network changes and troubleshooting by providing a high-level view of your entire network, making it easy to see connections, identify trouble spots, and navigate to device-level and port-level configurations. The solution also can be used to generate status reports, synchronize passwords, and upgrade software across all of your Cisco routers, switches, and access points.

Designed specifically for small organizations, Cisco Configuration Assistant provides graphical user interfaces to let you easily configure:

- Cisco Unified Communications Manager Express telephony features and phone extension services
- Cisco Unity Express voicemail
- Cisco router port settings and IP addresses
- Cisco router security, including router-based firewall and VPN services
- Cisco switches, including port settings, QoS, VLANs, and PoE services
- Cisco LAN security, including access control and identity services
- Cisco wireless and mobility services, including encryption, authentication, and guest access capabilities

Cisco Configuration Assistant is available for download at no charge at http://www.cisco.com/go/configurationassistant.

**Other Cisco Management Tools**

Small businesses can also take advantage of:

- **Cisco Network Assistant**: Cisco Network Assistant is a PC-based network management application optimized for wired and wireless LANs. The application was designed specifically for growing businesses with 40 or fewer switches and routers. Using Cisco Smartports technology, Cisco Network Assistant simplifies configuration, management, troubleshooting, and ongoing optimization of Cisco networks.
- **Cisco Monitor Manager**: Cisco Monitor Manager is a Microsoft Windows-based management application designed solely for the needs of small and medium-sized businesses. It monitors the network and collects network inventory and performance-monitoring data from the managed Cisco devices in the network.

## Services

Even when you are using the highest-quality network solutions, problems can still arise. In small businesses with limited networking expertise, even routine issues can quickly escalate, leaving applications offline and frustrating customers and employees. While your warranty will protect you against any defects in Cisco hardware and software, the reality is that most network issues result from the way the network has been configured or used, not from manufacturing defects. To protect your business and extend the value of your Cisco network investment, you should consider technical support services.

Cisco services available to small and medium-sized businesses include:

- Cisco SMARTnet® Service: Cisco SMARTnet Service is an award-winning technical support service that provides direct, anytime access to Cisco engineers, as well as extensive technical resources. The service provides rapid issue resolution, flexible device-by-device coverage, and premium service options to help you improve your operational efficiency and get the most from your Cisco investment.
- Cisco Smart Foundation Service: Designed specifically for small and medium-sized businesses, the Cisco Smart Foundation Service provides the easy, cost-effective network support you need to improve operational reliability, contain costs, and protect your

investment in Cisco networking solutions. The technical service offering provides access to Cisco technical engineers, who are specially trained to assist small businesses that do not have a dedicated networking staff. The service also includes advance hardware replacement, operating system software maintenance, and access to the Cisco Smart Foundation Service client and Web portal.

## Comprehensive IP Solutions for Small Businesses

When it comes to state-of-the-art IP applications and communications tools, small business owners no longer have to feel like they are on the outside looking in. Today, even the smallest companies can take advantage of the same IP-enabled productivity, efficiency, mobility, and cost benefits as large enterprises. Small companies face unique challenges and requirements, however, that any IP network solution must address. Enterprise-scale network solutions often are too costly and too complex to operate to benefit smaller businesses. At the same time, consumer-grade network solutions designed for use in the home cannot provide the security, performance, or rich feature sets that today's small businesses demand.

Fortunately, small businesses have a better option. Cisco network technologies for small and medium-sized businesses provide all of the IP capabilities that small companies need to compete and thrive in a global marketplace in affordable, easy-to-use solutions. Offering superior performance, security, reliability, and manageability, Cisco small-business IP solutions provide the tools you need to transform the way you work and communicate and build a more efficient, competitive business.

## For More Information

To find out more about Cisco IP network solutions for small businesses, visit http://www.cisco.com/go/smb.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C11-422624-00 09/07

 