

Cisco Network Foundation

A strong network foundation is the key to business agility and competitiveness in the technology-dependent Internet era. A Cisco® full service network foundation provides the intelligent services, including security, availability, and quality of service (QoS), that make it possible for companies to launch or optimize online applications, extend and manage operations more easily, streamline administration, and more.

Background

Today's small and medium-sized businesses are becoming more dependent on their existing network infrastructures to run their businesses efficiently and securely, serve customers more effectively, and work with partners and suppliers more easily. More companies are looking at new network technologies, such as IP communications and wireless, to further enhance business productivity and maintain a competitive advantage.

Faced with the challenges and opportunities of competing in the Internet era, growing companies must have confidence that their networks can support the evolution of their businesses. This requires more than simple assessment of capacity and equipment needs. Building an effective network infrastructure requires a comprehensive approach that both addresses current technology requirements and provides a framework for future applications and technologies.

Challenge

Building the right network infrastructure puts small and medium-sized companies in a powerful position to improve business resiliency and agility, enhance growth opportunities, lower the cost of operations, and increase employee productivity. However, it may not be clear what network strategy will yield the best results in both the short and long term.

Without the right capabilities in the network foundation, network administrators may waste time attempting to ensure solid security and maximum availability. And adding equipment or more capacity to get applications to work properly may result in inefficient use of corporate funds that offset productivity gains or lower cost of ownership goals.

Companies have much to take into consideration when fortifying and updating their networks. Following are some common questions and issues:



- *“How do I stop potential security breaches and ensure secure online transactions for my customers, suppliers, and employees without spending a fortune on network infrastructure?”*

Security breaches attack a company’s bottom line directly, by destroying valuable data and requiring substantial repair and recovery costs. Even the hint of security vulnerabilities can be damaging to a company’s reputation. Small and medium-sized businesses now recognize that they are just as vulnerable to devastating virus attacks and internal mishaps or mischief as large companies. Their challenge is to find a way to implement a secure network without driving up the cost of doing business.

- *“How do I keep recurring WAN connectivity costs down and response time up across the network?”*

As companies become more dependent on networked applications, just a few minutes of downtime can cost thousands of dollars in revenue as well as lost productivity. Similarly, poor response time can result in dissatisfied customers and erosion of a company’s image. Response time and network availability become an even greater concern as companies implement delay-sensitive IP communications and videoconferencing applications. Companies must find a way to maximize application and network performance without overspending on bandwidth.

- *“How do I extend network-based resources through wireless technology or IP communications without increasing security risks or making the network more difficult to manage?”*

A more mobile employee base can be enormously beneficial for companies trying to get the best leverage from a small workforce. By encouraging teleworking, keeping road warriors productive while traveling, and using wireless LAN (WLAN) technologies in the home office, companies can improve employee productivity and reduce the cost of doing business.

By using a converged network to carry voice and data over the same network (IP communications), companies can achieve incremental gains (saving on long-distance telephone charges) or major business transformations (introducing new multimedia-based services for customers). The challenge for small and medium-sized businesses is to incorporate these advantages into their organizations without negatively affecting their existing operations or increasing exposure to back-door security breaches.

Solution

The Cisco network foundation provides an effective way to address all of these challenges. A Cisco full service network solution helps ensure network security, reliability, and flexibility for existing applications, and provides a sound platform for adding new applications, features, and functionality in the future—at a pace that suits the needs of each individual business.

A full service, end-to-end network foundation is composed of the following major components:

- *Routers*—At the heart of a robust network foundation is the router, intelligently forwarding data packets from one network to another. Cisco has led the way in developing routers that incorporate the security, performance, reliability, and manageability features that companies need, including a range of routers specifically designed to meet the needs of small and medium-sized businesses. The breadth of Cisco router solutions also provides the flexibility for companies to use the most appropriate (and least expensive) WAN access technology, from cable to T1, for each location.



- *Switches*—Cisco Catalyst® Series intelligent Ethernet switches connect users directly to the network and serve as the primary path for traffic moving within and, in conjunction with the router, between networks. As more sophisticated business applications, higher volumes of traffic, and tighter security measures put greater demands on the network, Cisco Catalyst switches continue to evolve, giving companies greater intelligence and control without sacrificing the traditional simplicity of LAN switches. The broad family of Cisco switches also gives small- and medium-sized businesses more choices in configurations (standalone and stackable), speed (10/100/1000), and manageability.
- *Security devices*—The Cisco network foundation offers an end-to-end (including wireless and converged networks) security solution encompassing virtual private networks (VPNs), firewalls, intrusion detection systems (IDSs), and access control lists (ACLs). An integrated Cisco offering not only closes the security gaps associated with multivendor solutions—it is also more manageable, easier to support, and costs less to own. The modular approach Cisco takes to security enables small- and medium-sized businesses to add components, to scale, and to choose integrated solutions (routers with built-in firewall capabilities, for example) or dedicated devices as their business needs dictate. For example, companies can use the integrated firewall in Cisco routers or easy-to-manage, dedicated Cisco PIX® Firewall appliances. Cisco also offers both network-based and host-based IDSs for detecting intrusions on internal company networks.
- *VPNs*—Cisco VPNs provide secure connection between two different sites or locations on a network. This allows remote workers or branch sites to connect to the network with the peace of mind that no hacker or unwanted intruder will intercept their data. Cisco offers both integrated, router-based VPNs and standalone VPN concentrators and clients.
- *WLANs*—Cisco WLAN solutions enable employees in a facility or campus environment to access the company LAN without having a hard-wired connection. With Cisco Aironet® wireless technology, companies can eliminate most of the day-to-day challenges associated with moves, adds, and changes. Employees can move from cubicle to conference room and stay connected. They can sit in the lobby or the cafeteria and access the Internet or internal servers as though they were hard-wired to the high-speed Ethernet LAN. To ensure that WLAN transmissions are as secure as hard-wired transmissions, the Cisco Wireless Security Suite includes reinforced encryption and authentication. The combination of security capabilities in the Cisco Wireless Security Suite makes Cisco WLAN sessions virtually impossible to hack.

Benefits

The components of a Cisco network foundation individually deliver high value, but it is the full service network foundation—the combination and integration of routers, switches, security solutions, and WLAN devices—that enables the intelligent, end-to-end movement of data, voice, and video across networks. The Cisco network foundation ties together the people, products, and processes needed to help build a successful business by delivering intelligent services that provide the following benefits:

- *Integrated, end-to-end security*—To safeguard confidential business data, the Cisco network foundation employs enhanced security technology that protects the network from internal and external threats.
- *High availability*—The Cisco network foundation helps ensure reliable network access and maximum uptime. Designed to handle critical business applications for growing organizations, the Cisco network foundation includes support for network and link redundancy, dynamic routing, automatic failover, and redundant power for improved fault tolerance and network availability. Easy-to-use Web-based management helps keep administrative expenses down even as the network expands.



- *QoS*—The QoS features embedded in Cisco routers and switches classify, prioritize, and control network traffic, helping to ensure that time-sensitive applications such as voice and video are handled first, while lower priority applications continue to run reliably. QoS enables applications to perform better while maximizing network and bandwidth resources.
- *Service and support*—Cisco solutions are backed by the company’s award-winning technical support services, including over 1,600 CCIE® professionals in the field and global, follow-the-sun support. For more information, visit: www.cisco.com/en/US/support/index.html
- *Financing options*—The Cisco Systems Capital® program has created a comprehensive and exciting leasing program that makes it simple and easy to purchase networking equipment. The program provides complete financing solutions that can be customized to meet budget requirements and cash flow. For more information, visit: www.cisco.com/go/ciscocapital or www.smbleasingolutions.com

Next Steps

Cisco has designed a fast and easy way for companies of any size to evaluate whether their network foundation can support their Internet business strategy. The Cisco Internet Business Roadmap is an interactive tool that helps companies define their business goals, identify the appropriate e-business solutions to meet those goals, and get a customized Internet business roadmap on how to implement these solutions, including the essential network foundation. The roadmap is available at: www.cisco.com/go/cibr

As companies prepare to deploy additional applications and capabilities, the Cisco full service network foundation provides investment protection with a migration path for IP communications—and for productivity-enhancing wireless mobility.



Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, CCIE, Cisco, Cisco IOS, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)