

Cisco Mobile Office: At Home Corporate Home Office Solution





Executive Summary

Telework solutions extend a company's infrastructure to reach remote and home-based workforces, yielding corporate real estate cost reductions and enhancing employee productivity, satisfaction, and retention. The Cisco Mobile Office: At Home program helps businesses painlessly deploy telework solutions and shorten the time required to experience these benefits. As more employees work from home, companies can also look to connect them to the network. The program includes the Cisco corporate home office solution which combines high-speed access products for the home or remote workspace, security and quality of service (QoS) technologies to protect information over wide-area networks (WANs), and onsite assistance that can be tailored to a company's specific requirements and resource availability during the entire life cycle of the solution.

Cisco Corporate Home Office Solution Characteristics

Flexibility, manageability, security, and scalability characterize the Cisco corporate home office solution. Whether new to telework programs, or further extending existing services to home workers, companies can benefit from the Cisco suite of products and services. The Cisco corporate home office solution eases the transition from existing networks to extensible, telework-ready infrastructures. Each solution fulfills the unique business, process, and workforce objectives of an enterprise or small- to medium-sized business by incorporating:

High-Speed Access

- High-speed, reliable connectivity technologies to accommodate corporate-class applications
- Flexible broadband access options, including digital subscriber line (DSL), cable, and ISDN, to support virtually any residential service environment
- Support for wireless LANs (WLANs) and multiservice access devices such as IP phones

Business-Class Security and Performance

- End-to-end information and access protection through Cisco IOS® security services, virtual private network (VPN) and firewall technologies, and customer premises equipment (CPE) device-integrated security features
- Policy-driven service and access levels to meet QoS and service-level agreement (SLA) requirements

Rollout and Ongoing Maintenance Services

- Scalable, feature-extensible platforms to integrate emerging technologies and to support an evolving telework program
- Remote management capabilities, using Cisco IOS Software as part of an end-to-end Cisco solution
- A full complement of deployment services and support offerings, including planning, design, implementation, operational support, and optimization services that can be carried out in house or delivered by Cisco and its ecosystem of industry partners



Implementation Guidelines

Before reviewing the solution architectures and supporting technologies, IT organizations must make several key decisions about the telework program that they wish to implement. The following sections explain the issues that must be considered, with suggestions for accomplishing the related evaluations and analyses.

Step 1. Evaluate your in-house resources.

As this document describes, a complete telework solution involves the selection of not only appropriate access devices, but also the resources and expertise required to assess future user needs, install and provision in-home equipment, analyze and expand the enterprise infrastructure, identify and protect sensitive company data, maintain and update the extended infrastructure, and address technical support requests from all the teleworkers. Consider whether or not you have resources in house to accomplish all these tasks. Similarly, when analyzing and comparing the overall cost for your telework solution, be sure to include the costs associated with these other steps so that you are accurately comparing competitive offerings.

A Cisco account management team can provide valuable information regarding outsourced services. Based on your preferences, resources, and budget, the Cisco team will include a variety of Cisco partners that can offload your in-house staff, significantly shorten the deployment time, and ensure a high-quality, successful deployment. If desired, solution integration resources can be completely outsourced, in which case Cisco and its partners will take all the following steps for you.

If you decide that you have adequate in-house resources and wish to implement your telework solution without outsourcing, Cisco provides a variety of resources that will educate your team about the process and technologies involved in a telework solution implementation. For a summary of those resources, you can visit the Cisco Web site at: www.cisco.com/go/athome.

Step 2. Assess security requirements and practices.

Extending your corporate network to the homes of your employees underscores the need for security management. Do you already have firewall solutions and a comprehensive security plan in place?

Step 3. List desired services.

What types of services will your employees require? Does your business rely on videoconferencing? Are you planning to offer voice over IP (VoIP) services to reduce telecommunications costs? These types of services require guaranteed bandwidth and, therefore, indicate the need for QoS policies integrated into your telework solution.

Step 4. Survey connection choices in the coverage areas.

What connections are available from the local service providers for each employee that will be teleworking? Not all areas have broadband access. Consider ISDN lines in those cases.



Step 5. Survey the service providers in the coverage areas.

Determine which service providers operate in the areas populated by your teleworkers, and what types of services are available from each of those providers. You may want to start by surveying the service providers with which you have already established relationships. You might get a private DSL line per employee from one provider. Another might offer shared DSL lines and VPNs. Some providers are exclusively cable oriented. This survey process allows you to identify the types of in-home equipment that can be provided (for secure connections to your main office), and the areas where you will have to deploy CPE on your own. In some cases, you will be combining equipment from a local service provider with an additional CPE solution that can ensure the security that you require, or introduce QoS capabilities managed from your main office site.

Step 6. Select CPE options.

This planning guide includes an overview of the Cisco access solution offerings. Basically, you will be selecting CPE that meshes with your business practices and preferences. You can choose from:

- *Router-based solutions*—This one-box solution provides multiuser access for each site, built-in security features, and support for VPNs and QoS capabilities. Cisco routers can all be managed remotely, simplifying long-term management and support. Because routers must be configured, the telework solution must include adequate installation and provisioning procedures. If you order routers directly from Cisco, or if you work with a service provider that partners with Cisco, you can take advantage of the Cisco Express service to have preconfigured routers shipped directly to home sites (more information about Cisco Express is covered later in this document).
- *Hardware firewall solutions*—Dedicated hardware firewall appliances provide firewall functionality and also support VPNs.
- *Hardware-based VPN clients*—For the quickest setup and installation of a VPN, preconfigured hardware products may be the preferred solution. Depending on the applications that will be accessed at the corporate site, hardware VPN solutions sometimes provide higher throughput rates.
- *VPN software clients*—This product resides on each desktop or laptop PC. Software clients provide a low-cost solution, but are not as easily managed because they cannot be remotely accessed using all the available management and monitoring tools. These clients do not include firewall protection. They allow users to hook up to a WAN, but that connection requires further protection if it is to be secure.

Scalability will be the main decision driver. If you are starting small, the software-based client solutions offer a low-cost startup path. If you have a thousand teleworkers, an IT staff will find it difficult or impossible to troubleshoot PC-hosted software solutions, and a router-based solution will result in significant cost savings over the life of the deployment.



Step 7. Define corporate headquarters requirements.

The main office equipment required to support teleworker access will depend on the services available from the Internet service providers (ISPs) with which you will be working. If these ISPs deliver only Internet access, you will need some VPN termination or headend equipment to allow the telecommuters to securely connect to your main office. You may also need to implement your own firewall. Further sections in this document describe the product choices for these solutions.

Step 8. Perform rollout and provisioning.

Carefully consider the IT requirements for deploying CPE products. Many vendors offer seemingly low-cost products that require hours of configuration and setup time for each home site. If you will be sending your support team out to customer homes for installation or paying an outsourced team of installers, these routers can end up costing twice as much as the initial equipment cost.

Two Cisco offerings significantly reduce the rollout costs and deployment times for Cisco routers. Review the descriptions for the Cisco Router Web Setup tool and Cisco Configuration Express service. If your telework solution will extend enterprise resources to large numbers of teleworkers, these timesaving tools and services will lower the overall cost of ownership for your teleworker solution. The IT staff at headquarters can also be saved the efforts required to handle CPE equipment if your service provider supports these Cisco solutions.

Step 9. Plan for ongoing maintenance and updates.

Your Cisco account team can take advantage of their experience with other telework solutions and ensure that your deployment will be adequately maintained and updated, maximizing your return on investment for this project. They can advise you about outsourcing support, or taking advantage of Cisco resources such as:

- Cisco Secure Policy Manager—This tool manages and monitors security policies across Cisco products.
- Cisco PIX[®] Device Manager—This tool similarly addresses Cisco firewall solutions.
- Third-party software tools—Cisco partners offer solutions for monitoring policies and products throughout an enterprise and teleworking infrastructure.

After you deploy a telework solution, you will need a designated IT contact to be responsible for monitoring and maintaining user connections. Teleworkers will also need defined level 1 and level 2 support channels, including whom and where to call with their needs. Cisco can recommend partners for outsourcing these aspects of the solution and help you analyze the potential cost savings associated with outsourcing options.



Solution Architectures

Figure 1 Cisco DSL Router with VPN Solution

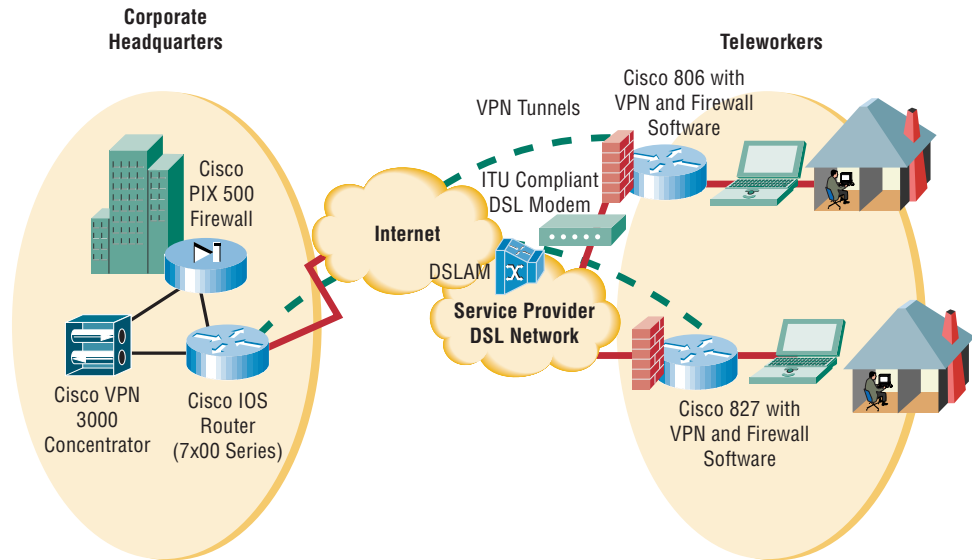


Figure 2 Cisco Cable VPN Solution

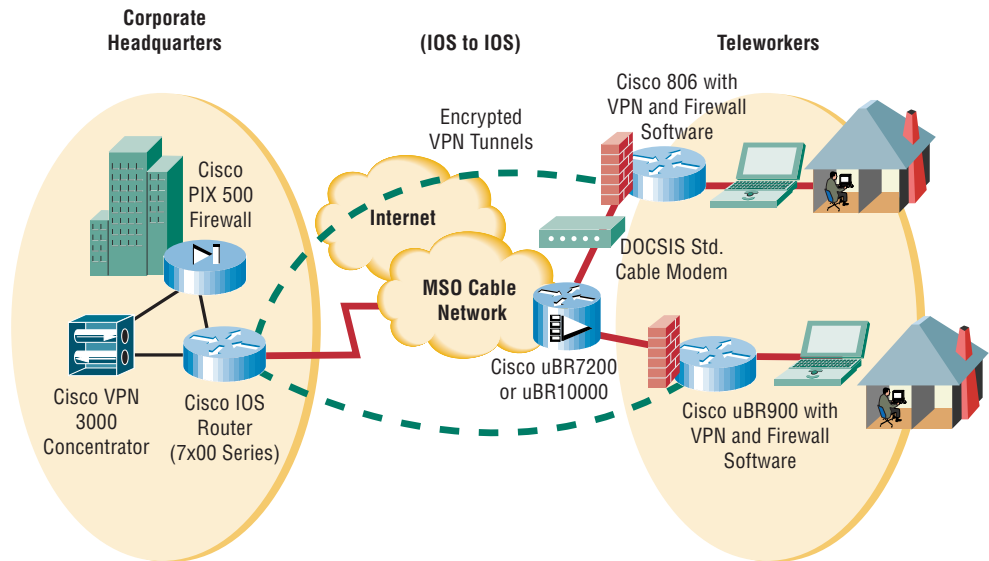
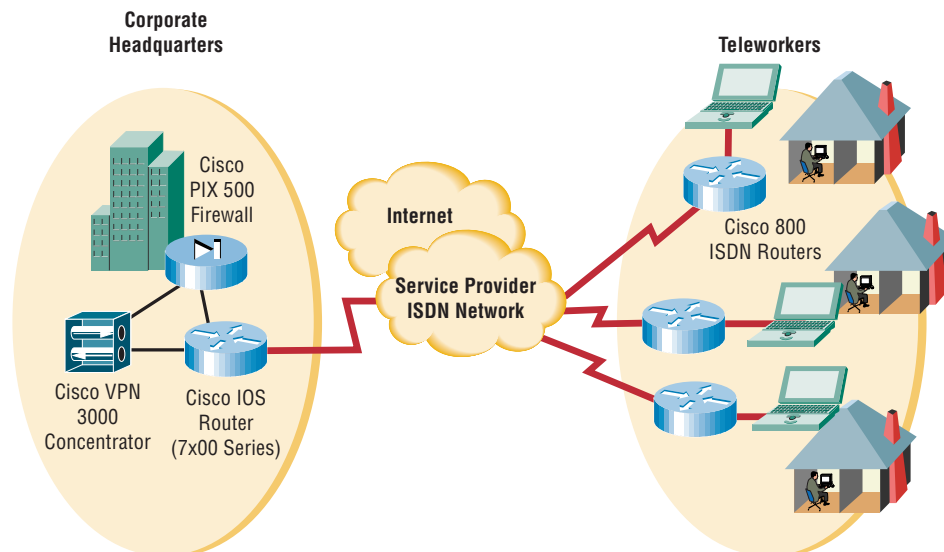




Figure 3 Cisco ISDN Solution



Figures 1, 2, and 3 illustrate how the Cisco CPE solutions fit into the entire Cisco corporate home office architectures for DSL, cable, and ISDN access, respectively. These solution architectures demonstrate the flexibility of the Cisco corporate home office solution for a variety of corporate requirements and worker service environments.

DSL Access

The affordability of DSL makes it a popular telework access technology. DSL lines offer always-on connectivity and provide varying levels of bandwidth. Figure 1 illustrates the deployment of a DSL router solution (based on the Cisco 827 asymmetric DSL [ADSL] router) configured with VPN and firewall software. This one-box CPE solution requires only a DSL line to the teleworker's home.

A DSL service provider can provide both the DSL line to the home as well as connectivity to the Internet. Alternatively, the Cisco corporate home office architecture can include a point-to-point configuration utilizing a private DSL connection. This inherently secure solution does not require a VPN and adds service levels in the service-provider network for voice, video, and mission-critical applications.

In some instances, the DSL service provider may not offer a Cisco DSL router. A broadband modem may be the only CPE offered to the teleworker. If this is the case, a Cisco 806 router can be connected to the DSL modem to gain business-class security, VPN features, Cisco IOS remote management capabilities, and QoS features. Another choice is to use a hardware-based security appliance such as a Cisco PIX Firewall or VPN hardware client.

Cable Access

Widely available to teleworkers, cable access offers higher bandwidth than dialup connections. Cable operators and service providers use a cable access router such as the Cisco uBR 900 Universal Broadband Router Series to deliver the service to residential subscribers. As shown in Figure 2, the Cisco uBR 900 provides the required VPN/firewall transmission and access protection software. Cisco broadband cable solutions



are highly manageable through Cisco IOS Software and can include QoS support for voice, video, and other multiservice applications.

As with DSL, a Cisco cable router may not be offered by the cable operator. A simple cable modem may be the only deployment option extended to the teleworker. To add security, VPN, remote management, and QoS features, a Cisco 806 can be connected to the cable modem through the router Ethernet WAN port. Likewise, customers may choose to implement a hardware security appliance such as a Cisco PIX Firewall or Cisco 3002 Hardware Client.

ISDN Access

For homes that do not have access to DSL or cable Internet access services, ISDN is another connection option. Several Cisco router solutions, combined with a private ISDN line, offer highly secure and high-speed access to a remote network.

The Foundation for Growth

The Cisco corporate home office solution is architected not only to deliver immediate telework benefits but also to provide the foundation for building higher-function infrastructures to meet expanding corporate needs and to incorporate technology advances. Cisco router-based solutions include QoS features that allow companies to eventually extend IP phones to home-office workers. And, when the company makes the effort to extend security to the home office, the Cisco portfolio of corporate home office products includes wireless LAN products that do not compromise the security investment.

Cisco High-Speed Remote Access Solutions

Home-office workers can be connected to the corporate network in many ways. Companies should consider not just the features of the equipment of the home office but also how that equipment is to be managed and deployed. Likewise, there are choices for the equipment used at the main office. The Cisco corporate home office solution enables home-worker access to corporate services via DSL, cable, and ISDN lines. For added flexibility and a smooth transition to future services, the Cisco corporate home office solution architecture can also support wireless LAN (WLAN) connectivity and multiservice access products (for devices such as IP phones). By taking advantage of the latest Cisco CPE devices, a Cisco corporate home office solution can be deployed economically, quickly, and with a compact footprint to ensure suitability for the home setting.

Router-Based Solutions

Cisco home-office routing solutions provide flexible choices to address the full range of user requirements.

Cisco 800 Series Routers

The Cisco 800 Series of fixed-configuration routers provides enhanced security, low cost of ownership, proven reliability, and safe investment through the power of Cisco IOS Software tailored for small offices and telecommuters.



Table 1 Cisco 800 Series Models

Model	WAN	Ethernet	Analog Telephone Ports
DSL			
Cisco 802 IDSL	One IDSL U, integrated NT1	One 10BASE-T	None
Cisco 804 IDSL	One IDSL U, integrated NT1	10BASE-T (RJ-45) four-port hub	None
Cisco 827	One ADSL interface	One 10BASE-T	None
Cisco 827-4V	One ADSL interface	One 10BASE-T	4 analog telephone foreign exchange station (FXS) Ports
ISDN			
Cisco 801	One ISDN Basic Rate Interface (BRI) S/T	One 10BASE-T	None
Cisco 802	One ISDN BRI U, integrated NT1	One 10BASE-T	None
Cisco 803	ISDN BRI S/T	10BASE-T (RJ-45) four-port hub	Two (RJ-11) Analog Telephone Ports
Cisco 804	ISDN BRI U, integrated NT1	10BASE-T (RJ-45) four-port hub	Two (RJ-11) Analog Telephone Ports
Cisco 801 CAPI	One ISDN BRI S/T	One 10BASE-T	None
Cisco 803 CAPI	ISDN BRI S/T	10BASE-T (RJ-45) four-port hub	2 (RJ-11) Analog Telephone Ports
Serial			
Cisco 805	One smart serial port for sync or async dial up	One 10BASE-T	None

The newest addition to the Cisco 800 Series has been designed specifically for broadband connection. The Cisco 806 Broadband Gateway Router combines business-class functionality with broadband access for small offices and corporate teleworkers. The software-upgradable platform delivers multiuser access over a single broadband connection. The Cisco 806 connects to a broadband modem through an Ethernet port, giving enterprises the option to standardize on a single secure, manageable device—whether the broadband service uses DSL, cable, Ethernet, or Long-Range Ethernet (LRE)—for user connection to the corporate network. With built-in Cisco IOS Software, the Cisco 806 Router combines enterprise-class security and QoS capabilities with remote management features tailored to home environments. Enterprise-ready security features include data encryption for VPNs (which allow secure

communications over a public infrastructure such as the Internet) and a stateful inspection firewall for perimeter security.

For more information on the Cisco 800 Series routers, visit: www.cisco.com/warp/public/cc/pd/rt/800/

Cisco Router Web Setup

The Cisco Router Web Setup (Cisco RWS) tool provides a graphical user interface (GUI) for configuring Cisco 800 DSL routers, Cisco 806 routers, and Cisco SOHO 70 Series Small Office/Home Office routers, allowing users to set up the router quickly and easily. Users without knowledge of how to configure a Cisco 827 ADSL Router with the Cisco IOS command-line interface (CLI) can use the Cisco Router Web Setup tool to configure the router in just a few simple steps. With this tool, Cisco 800 and SOHO 70 Series customers can take advantage of the power of Cisco IOS Software



without the technical skills typically needed for router configuration. The Cisco Router Web Setup tool gives users the following benefits:

- Simplified setup
- Implementation of advanced configuration features
- Router security
- Router monitoring

Cisco SOHO Routers

The Cisco SOHO 70 Series provides an affordable, secure, multiuser DSL access solution for small- and home-office customers while reducing deployment and operational costs for service providers. Through the power of Cisco IOS Software technology, the Cisco SOHO 70 Series ADSL and G.SHDSL routers provide superior manageability and reliability:

- Affordable, multiuser access with a single DSL line
- Internet security with packet-filtering firewall
- Easy setup and deployment with Web-based configuration
- Remote management with the power of Cisco IOS Software
- Proven reliability

For more on the Cisco SOHO Series of routers, visit: www.cisco.com/warp/public/cc/pd/rt/70/index.shtml

Cisco uBR 900 Series Cable Access Routers

The Cisco uBR 900 Series delivers high-function cable broadband access. Incorporating a fully integrated Cisco IOS router and CableLabs-certified cable modem, the device interoperates with any bidirectional, CableLabs-qualified cable modem termination system (CMTS). Security features include support for IP Security (IPSec) VPNs and firewall protection.

For more information on Cisco uBR 900 Series cable access routers, visit: www.cisco.com/warp/public/cc/pd/rt/900/

Meeting the Security and QoS Performance Challenges of Telework Deployments

Security

The breadth of the Cisco security offering allows flexibility in the design and level of security implemented in corporate telework programs. The Cisco corporate home office solution incorporates a variety of devices, software, and services. Cisco also offers a security blueprint: Cisco SAFE. Based on Cisco AVVID (Architecture for Voice, Video and Integrated Data), Cisco SAFE addresses the entire enterprise, including teleworkers, and determines which security solutions should be included and deployed throughout a network. Via uniquely designed modules that simplify security design, rollout, and management as networks evolve, the Cisco SAFE blueprint handles the distinct requirements of each network area. Each module may include Cisco security functionality such as:

- Firewalls
- Intrusion-detection and scanning systems
- Device and user authentication
- Antivirus technologies
- Encryption
- Tunneling
- VPN capabilities

The blueprint eliminates the need for redesign of the security architecture as new services such as teleworking are added.

The Cisco corporate home office solution ensures enterprise security by implementing edge-to-core security with data and access protection, including secure WLAN access, for every home user. Engineering design for all Cisco security solutions achieves information delivery and access protection without any performance trade-off.



Cisco VPN Technology

VPNs use the public Internet infrastructure to establish inherently secure, private network connections between two points (between the CPE and the corporate IT infrastructure in the case of a telework solution). Technically, encrypted tunnels can be authenticated and terminated on a variety of platforms, including firewalls, routers, PCs (using software), and purpose-built VPN devices. Cisco VPN solutions, based on Cisco AVVID, span a broad spectrum of functionality and format, ranging from VPN-optimized routers and firewalls to dedicated VPN concentrators. Each platform has associated benefits, depending on the connectivity challenge. The Cisco corporate home office solution tailors an appropriate complement of products and technologies to meet specific security requirements of each business environment.

The Cisco corporate home office solution gives consideration to the essential aspects of user authentication and VPN security functionality, including the IPSec framework, encryption, and tunneling protocols. Cisco security components, for example, can support:

- The IPSec standard for securing IP traffic
- Triple Data Encryption Standard (3DES), the highest level of encryption currently available
- Layer 2 and Layer 3 tunneling

Cisco VPN Products

At the enterprise site, the Cisco VPN 3000 Concentrator Series scales to deliver up to 100-Mbps 3DES encrypted throughput. Integrated VPN support is available on Cisco routers, Cisco firewall and VPN appliances, and VPN software clients.

For more on the Cisco VPN 3000 Concentrator Series, visit: www.cisco.com/warp/public/cc/pd/hb/vp3000/

Cisco Firewall Products

Firewall technology secures the network perimeter of a given site. The Cisco IOS Firewall Feature Set, implemented, for example, with the Cisco 806 Broadband Gateway Router, incorporates numerous key functions to maintain this security. Functions include:

- Per-application dynamic access control (stateful inspection) for all traffic across perimeters
- Defense and protection against denial-of-service attacks
- Packet-header checks
- Protection against malicious Java applets
- Detailed transaction reporting on a per-application, per-feature basis

Other basic Cisco IOS Software security services include:

- Access control lists (ACLs)
- Network/Port Address Translation (NAT/PAT)
- Lock and Key
- Dynamic ACLs
- Router and route authentication
- Generic routing encapsulation (GRE) tunneling

Cisco Secure PIX Firewall

This dedicated firewall appliance delivers strong security for telework applications. It creates minimal to no network performance impact. The Cisco Secure PIX 506 Firewall product enforces secure access between an internal network and Internet, extranet, or intranet links. Available in five models, the firewall scales to accommodate a range of network sizes and business requirements.



QoS for Future Applications

In addition to bullet-proof security, delivering enterprise-class services to home-based workers requires the integration of QoS functionality, including the ability to define, maintain, and monitor required levels of services. QoS capability is essential for services with high-bandwidth requirements, such as services involving voice, video, and other mission-critical applications.

Cisco IOS Software on Cisco routers incorporates the needed QoS features to effectively manage latency-sensitive traffic, enabling applications such as videoconferencing and IP telephony and offering potential savings through the reduction of telephone toll charges. QoS functions enable prioritization of traffic—for example, giving higher priority to a voice application compared to someone Web surfing—and very efficient bandwidth allocation. Key IP QoS features include low-latency queuing, Weighted Random Early Detection, and committed access rate. These features ensure consistent response times for multiple applications, allow application classification, and minimize congestion.

The Rollout Process: In-House or Outsourced Resources

The Cisco Mobile Office: At Home Program goes beyond access technologies, hardware, and software. Successful telework programs require an experienced team that can:

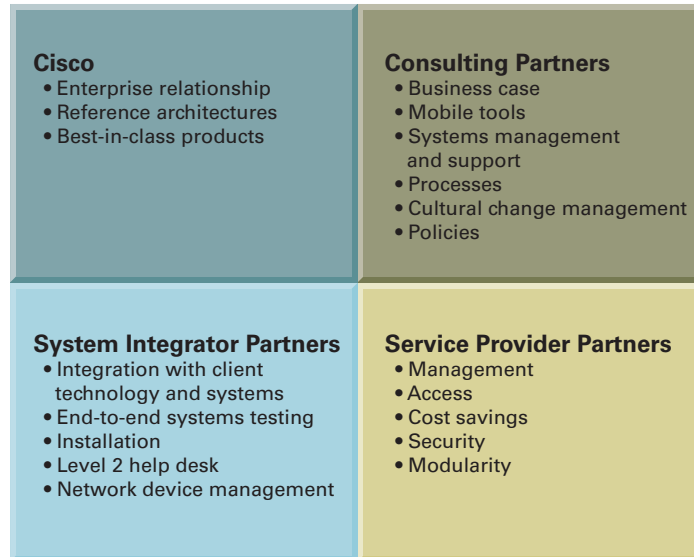
- Analyze the requirements
- Define a specific implementation plan
- Coordinate installation and provisioning of the required WAN links and CPE
- Install the necessary software
- Initiate services
- Outsource as appropriate for Internet service and other required capabilities
- Design and implement user training

If you have an experienced team in house, you can shorten your rollout time and avoid some pitfalls by taking advantage of the resources on the Cisco Mobile Office: At Home web site. Simply visit www.cisco.com/go/athome.

If you have limited in-house resources or your team lacks the expertise required to quickly and cost-effectively implement a successful telework program, you can take advantage of out-sourced resources. Cisco takes advantage of the company's best practices for in-house telework solutions to assist you in identifying the areas that require additional resources, locate the appropriate outside resources, and integrate these resources into the overall Cisco telework solution to maximize your investment and business benefits.



Figure 4 Cisco Mobile Office: At Home Program—An Ecosystem Approach



Cisco has partnered with a variety of companies to provide the consulting services, service providers, and system integration that are necessary to deploy a corporate-wide teleworking solution.

Consultants

Consultants can help:

- Analyze and document the business case for real estate cost savings and productivity benefits of the proposed Cisco corporate home office solution
- Resolve HR and cultural issues that may arise when introducing teleworking solutions in a company
- Define the overall technology solution, based on the desired application access for the appropriate job roles
- Specify the required PC technology and remote configuration processes
- Design an appropriate service and support model for the rollout
- Identify those employees best suited to roll out to a telework center or home office

Service Providers

- Service providers can provide:
- High-speed access into the home, including DSL, cable, and ISDN
- Line provisioning
- A single point of contact for managed VPNs, and other business-class services including SLAs and QoS to support VoIP
- Installation, deployment, and management of CPE in the home
- Level 1 and level 2 support 24 x 7
- In some cases, system integration services

Systems Integrators

After the rollout plan is in place, the systems integration phase begins. A systems integrator will provide the internal processes for employees to sign up for the telework solution, including ordering line provisioning, process integration, installation, and service and support into the home office. In addition, the systems integration provides for technology integration across the

standardized platforms that employees will use in their homes, including end-to-end testing on the remote work solution. The system integrator can also provide remote installation at the employee home, if needed, ongoing level 2 support for the enterprise, and management of the VPN services.

Cisco and Cisco Certified Partners

Together with these partners, Cisco can provide the comprehensive portfolio of products and services required to deploy an end-to-end telework solution. Cisco Certified Partners serve as an extension of the Cisco team. Partners participate in in-depth technology and product training, and receive Cisco's latest tools and collateral, including access to the online return-on-investment (ROI) calculator, the corporate home-office Web site, and Cisco's work-at-home best practices.

Service and Support

The Cisco Mobile Office: At Home program is supported by a service portfolio designed to align the customers' unique business strategies and goals with high performance, high availability corporate home office solutions. Technical Support Services and Security Services covering the entire product life cycle are delivered by Cisco and its ecosystem of best-in-class partners. Technical Support Services such as SMARTnet™ and Software Application Support/plus Upgrades are available maximize operational availability. Security/VPN Specialization Partners specializing in the design and installation of network security solutions are available assist in deploying secure network solutions.

Service Information Links

Information on SMARTnet:

www.cisco.com/warp/public/cc/serv/mkt/sup/ent/snet/

Information on Software Application Service/plus Upgrades:

www.cisco.com/warp/public/cc/serv/mkt/sup/ent/soft/index.shtml

Information on Security Partners:

www.cisco.com/warp/public/779/largeent/partner/esap/secvpn.html



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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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: 65 317 7777
Fax: 65 317 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 © 1992–2001 Cisco Systems, Inc. All rights reserved. SMARTnet is a trademark; and Cisco, Cisco IOS, Cisco Systems, 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. (01110R) 02/02 7929BW