Disaster Preparedness: Maintaining Business Communications During Unexpected Events

Using the network to deliver remote employee communications that enable business continuity during disasters and pandemics

Summary

Disaster planning has become a core component of business continuity planning. A disaster or pandemic event can have a profound impact on business operations. Primary among those issues is the displacement of workforce from the worksite. If a disaster or pandemic takes place, employees will not be able to access the worksite for several days, weeks, or even months. Without a plan for remote working solutions for displaced workers, an organization may not be able continue operations, thus crippling the business.

Cisco® offers complete remote working solutions that enable employees to work with all the resources of their office environment by extending the network data, applications, and phone services available at the worksite to employees' homes or alternate work locations. Cisco remote working solutions deliver a complete suite of data, voice, and video services to teleworkers' desktops. Features include:

- Enables employees to work from home or an alternate work location and perform their jobs with the same efficiency and productivity as their office environment
- Delivers great flexibility in remote working environments, from work-at-home solutions using company-owned laptop PCs or employee-owned PCs to using public Internet terminals or Internet-enabled mobile phones
- Provides comprehensive, integrated security, including customized access levels based on user, access device, and location
- Minimizes equipment required at employee locations; can use existing network infrastructure and IT processes for service deployment
- Provides streamlined, "low-touch" remote user provisioning and management

Scoping and Preparing for The Unexpected

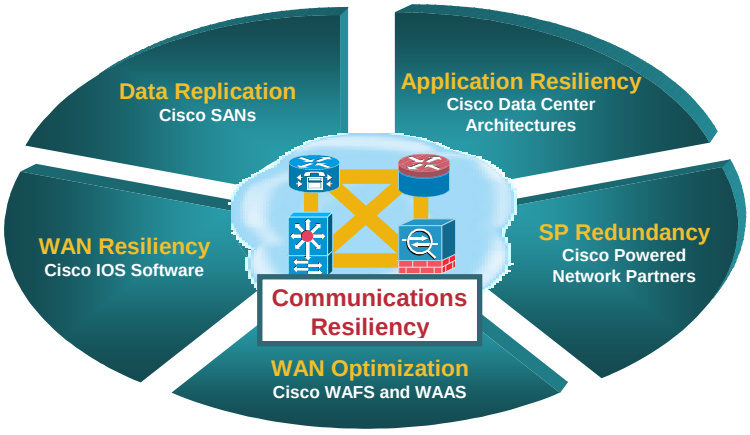
Many types of events can keep employees from being able to access the worksite. Some are top of mind, such as flu pandemics or natural disasters. But a displacement event can be something as ordinary as a transit strike or a bridge failure that prevents commutes. The reality is many events can keep employees from accessing the workplace—and they are nearly impossible to predict. The best strategy is to be prepared: to have an infrastructure in place, tested, and ready for when an employee displacement event occurs.

When preparing the IT infrastructure for business continuity, it is important to realize that different disaster events require different approaches to preparing the IT infrastructure. Broadly, there are two types of employee displacement events:

1. An event that impacts infrastructure and property, such as an earthquake or terrorist attack. These events can damage or destroy the worksite and the network assets that exist there.
2. An event that leaves the worksite and network assets in place, but blocks employee access to the worksite. Examples include pandemics and transit strikes.

Dealing with workplace damage or destruction requires a broad IT business continuity plan. Cisco offers solutions in each of the salient areas. If the IT infrastructure sustains damage, considerations for application resiliency, WAN connectivity resiliency, data replication, and accessibility must be considered (Figure 1). If the event leaves the IT infrastructure in place, then the problem is primarily focused on enabling remote working for the displaced employees.

Figure 1. Data and Voice Communications Resiliency—the Network Fabric for Any Business Continuity Planning



In any disaster preparedness case, “communications resiliency”—the ability to continue providing data and voice services to all aspects of the organization—is the core of any IT business continuity plan. It provides the network connectivity fabric for all IT services. Whether the workplace is destroyed or employees simply cannot go to the office, having a communications plan for enabling employees to perform their job roles from an alternate work location is critical. To maintain business operations the workplace has to move to wherever the employee is working from until the displacement event is rectified. In most cases this will be employees’ homes.

Bringing The Workplace To The Employee

Many of today’s job functions require access to applications and data that reside on the organization’s IT network, as well as a business telephone. In the office location, services such as e-mail, instant messaging, client/server applications, file servers and databases, the organization’s intranet, Internet access, phone service, and voicemail are taken for granted. But even for employees with laptop computers at their disposal, most of these services are not available outside the office unless specific network solutions have been deployed. And for employees who work at fixed workstations, they cannot perform their job duties at all when away from the office. To ensure business continuity during disaster or pandemic events, it is critical to enable fully functional virtual offices for their workforce.

Providing seamless communications to a displaced and dispersed workforce during a disaster or pandemic requires a portable, extendable communications infrastructure. Key steps in building such an infrastructure are:

- Categorizing job roles in the organization by communications requirements. Different job roles require different levels of communication to be productive.
- Surveying the existing IT infrastructure and its remote communications capabilities. Can it reach all employees whose roles are required for operation of the business? Can it handle capacity in the event of mass employee displacement? Does it address employees who may not have a company-provided laptop?
- Is the remote communications infrastructure deployed? Is it tested, both from an IT operations standpoint as well as a business process standpoint? Is the solution staged for employees who may not have access to remote communications as a part of their normally deployed IT services (employees who don't already have remote-access VPN, for example)?

Cisco Disaster Preparedness Solutions – Full-Function Remote Working Environments

Cisco provides a full suite of VPN and voice over IP (VoIP) solutions that enable employees with just a laptop computer or no company computer at all to recreate their office resources at their home or other Internet-enabled location. Using VPN services, employees can securely access all data applications—such as e-mail, instant messaging, client/server applications, file servers and databases, and intranet services—from a remote working location. Furthermore, the VPN connection can be used to extend voicemail or even employees' office phone extensions directly to their PC or to an IP phone handset, thereby fully replicating the office location at a remote virtual office.

VPN and VoIP Technologies Defined

VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with today's VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, anytime.

VoIP, also known as IP telephony, is a technology that enables transmission of voice communications over the Internet or other IP networks. VoIP services provide highly mobile voice services; they can be follow the user anywhere an Internet connection is available.

When moving work to the employee, there are three main approaches available based on the communications needs of individual employees as required to perform their job functions:

- **Remote data application access:** Provides users access to e-mail, instant messaging, client/server applications, file servers and databases, and intranet services from their company laptop computer using remote-access VPN services. This is appropriate for "back-office" employees who do not often meet or collaborate with fellow employees or customers in real time. Most communications are conducted via e-mail or instant messaging.

- **Remote data application and office phone extension access:** Uses the remote-access VPN connection to provide users with access to their office phone extension via a PC-based IP phone, as well as the broad data applications access as noted above. This is appropriate for employees who meet or collaborate with fellow employees. Communications can be conducted in real-time conversations via employees' office phones, as well as over e-mail or instant messaging.
- **Full office replication:** This approach duplicates an employee's office at home or another designated location using site-to-site VPN technology. It delivers business-quality voice communications as enabled by the higher-quality transmission capabilities of site-to-site VPN technology, as well as a standard IP phone handset. Using the high-quality site-to-site network connection, video conferencing is also enabled by this solution. This approach also delivers full data applications access.

Identifying the communications tools required for each job role to enable continuity of business operations when displaced from the office is critical to building a disaster-ready communications infrastructure. "Right-sizing" the solution for the job role increases employee business productivity during a displacement event, while minimizing IT deployment and management costs associated with the solution.

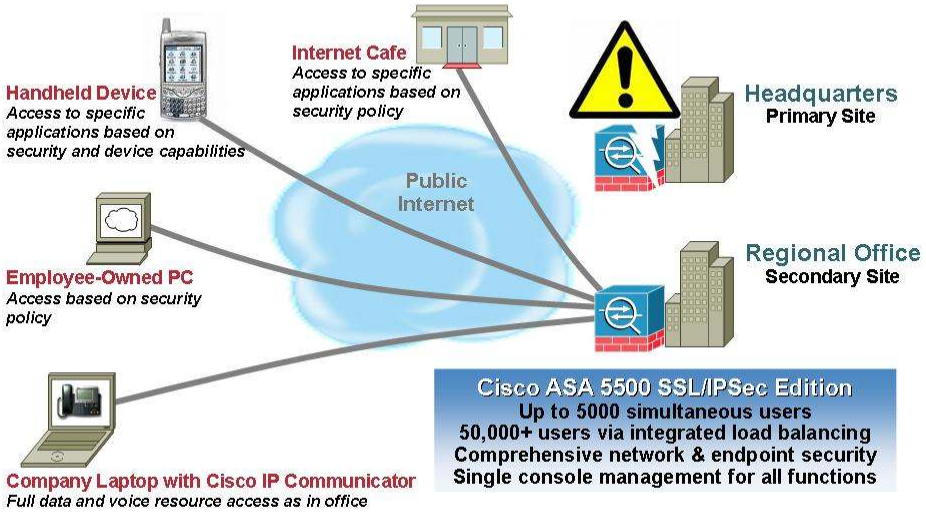
Each of these approaches can be addressed with a combination of Cisco VPN, Unified Communications, and remote collaboration technologies as delivered through the Cisco Anywhere Office and Cisco Enterprise Class Teleworker communications resilience solutions. Each of these solutions is customizable to the specific requirements of the job role, thus maximizing employee productivity while minimizing IT cost.

Cisco Anywhere Office: Remote Data and Data+Voice Access

The Cisco Anywhere Office solution enables employees to turn their company-provided laptops into fully functional offices from any Internet-connected location. Built on Cisco remote-access VPN technologies, the Anywhere Office enables employees to connect remotely to the company network for access to virtually any application or network resource. Employee office phone extensions may also be extended over the VPN using Cisco IP Communicator for full data+voice services from the employee laptop. Cisco IP Communicator is PC software that uses VoIP technology to extend company voice services to employee computers.

Cisco Anywhere Office may also provide data connectivity to employees without company-provided laptops. Again, using Cisco remote-access VPN technologies, secure network access is extendable to employee-owned PCs, public Internet terminals, and Internet-enabled wireless devices such as smartphones (Figure 2).

Figure 2. Cisco Anywhere Office Provides Remote Data and Voice Connectivity



Remote-Access Vpn Connectivity For The Cisco Anywhere Office

The foundation of the Cisco Anywhere Office is the remote-access VPN technology that provides the “pipe” back to the company network. The main considerations when providing remote network access are:

- Ensuring access and data is secure across the remote link and on the remote desktop
- Providing an appropriate level of network access based on user, access device, and access location
- Enabling access from diverse devices such as employee-owned computers and wireless devices, as appropriate
- Minimizing provisioning and management processes; no dependence on end users for configuration and management
- Providing scalability, performance, and resiliency to dependably connect remote users during the connection “bursts” characteristic of disaster scenarios

There are two primary methods for deploying remote-access VPNs: IP Security (IPsec) and Secure Sockets Layer (SSL). Each method has its advantages based on the access requirements of users and the organization’s IT processes. While many solutions only offer either IPsec or SSL, Cisco remote-access VPN solutions offer both technologies integrated on a single platform, such as the Cisco ASA 5500 Series SSL/IPsec VPN Edition or Cisco routers that offer with unified management. Providing both IPsec and SSL technologies enables organizations to customize their remote-access VPN without any additional hardware or management complexity.

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. They do not require any special-purpose client software to be pre-installed on the system; this makes SSL VPNs capable of “anywhere” connectivity from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, shared Internet terminals, and Internet-enabled mobile phones. Any software required for application access across the SSL VPN connection is dynamically downloaded on an as-needed basis, thereby minimizing desktop software maintenance.

IPsec-based VPNs are the deployment-proven remote-access technology used by most organizations today. IPsec VPN connections are established using pre-installed VPN client software on the user desktop, thus focusing it primarily on company-managed desktops.

Both IPsec and SSL VPN technologies offer access to virtually any network application or resource. SSL VPNs offer additional features such as easy connectivity from non-company-managed desktops, little or no desktop software maintenance, and user-customized Web portals upon login. And Cisco remote-access solutions offer scalability for any size deployment—from 10 to 5000 simultaneous users per device and 50,000+ simultaneous users per cluster of VPN gateways. Cisco's unmatched VPN scalability and resiliency helps ensure that users will be able to access the VPN when they need it.

Securing The Anywhere Office

Ensuring employees are granted access to the appropriate network resources across the remote-access VPN is necessary for a secure remote working solution. Cisco remote-access VPN solutions can tailor employee access based on user device, location, endpoint security posture, and other criteria. This security feature protects an organization's data by providing granular access control to specific Webpages, network server directories, and files. Once an employee is granted appropriate access, protecting the data they bring from the network to their desktop is the next critical step. Again, based on user device, location, endpoint security posture, and other criteria, Cisco remote-access VPN solutions help ensure that this data is handled according to the organization's data security policy. Data downloaded to endpoints via e-mail, file transfers, or any other mechanism during the VPN session can be automatically erased at the end of the VPN session without any user input.

Protecting the network from worms, viruses, spyware, hacking, data theft, and application abuse during a disaster, especially when broad teleworking is in operation, is paramount for ensuring network and resource availability. Remote-access VPN connectivity is a common point of entry for such threats, due to how VPNs are designed and deployed. For both new and existing IPsec and SSL VPN installations, VPNs are often deployed without proper endpoint and network security. Cisco remote-access VPN solutions offer threat-protected VPN services with full firewall, antivirus, anti-spyware, intrusion prevention, application control, and full endpoint security capabilities. These security services are integrated into the VPN platform, delivering a threat-protected VPN solution without any additional equipment, design, deployment, or operational complexity.

Voice Services For The Anywhere Office

A unique feature of the Cisco Anywhere Office is the ability to extend the employee's phone extension from the office location to the employee's alternate working location. Using Cisco IP Communicator, employees can place and receive calls from their PCs using the same telephone number as exists in their office location (Figure 3). This business phone portability is key to maintaining communications during a disruptive event; it makes communications with employees as seamless as if they were actually sitting in the office.

Cisco IP Communicator is a Microsoft Windows-based application that is easy to deploy and features some of the latest technology and advancements available with IP communications today. When using Cisco IP Communicator remotely, users are not just taking their office phone extension with them—they also have access to the same familiar phone services they have in the office. This advantage boosts business collaboration and responsiveness, and helps organizations keep pace with today's mobile business environment.

Figure 3. Cisco IP Communicator Running on a PC

Cisco IP Communicator uses the Cisco Unified CallManager call processing system to provide advanced telephony features and VoIP capabilities. When registered to Cisco Unified CallManager system, Cisco IP Communicator has the capabilities of a full-featured Cisco Unified IP Phone, including the ability to transfer calls, forward calls, and conference additional participants to an existing call. This means that system administrators can provision Cisco IP Communicator as they would any other Cisco Unified IP Phone, greatly simplifying IP phone management.

Cisco IP Communicator offers the following flexible user communication interfaces:

- **Headset Mode**–Offers the highest-quality voice communications capabilities.
- **Handset Mode**–Interoperates with third-party USB telephony handsets.
- **Speakerphone Mode**–Converts a computer into a half-duplex, hands-free speakerphone

Cisco IP Communicator provides a mobile-quality telephony experience suitable for business communications. Advanced voice quality technologies such as jitter buffering, echo suppression, noise cancellation, and silence suppression preserve call quality even when underlying network conditions may vary.

Managing The Cisco Anywhere Office

Centralized VPN management streamlines configuration and updating of remote users in real time. All IPsec and SSL VPN configuration policy is centralized on the VPN gateway and pushed to the user on an as-needed basis. VPN configurations can also be locked down on the remote user desktop, thereby eliminating the risk of users invalidating the VPN configuration or violating security policy. VPN and security policy can be configured directly on the VPN gateway using an integrated Web-based device manager or the multidevice VPN management console, Cisco Security Manager. This centralized management model eliminates the user from the configuration or support equation.

Management of Cisco IP Communicator voice services are also centralized, with all configuration parameters pushed from the Cisco Unified CallManager call control platform. This management schema makes Cisco IP Communicator as transparent to manage as any IP phone on the network.

Building The Cisco Anywhere Office

Deploying the Cisco Anywhere Office solution requires the following components:

- **Remote access VPN for data connectivity:** A Cisco VPN gateway such as the Cisco ASA 5500 Series adaptive security appliance or a Cisco router. If using IPsec VPN, the Cisco VPN Client must be installed on employee desktops. If a Cisco remote-access VPN gateway is already installed, providing teleworking services during a disaster or pandemic is primarily a matter of ensuring adequate simultaneous user capacity in the event of a large employee displacement and ensuring flexible end-user device access (from an employee-owned PC, for example) via SSL VPN services. Most VPNs are sized to support 10 percent of the workforce at any one time. During a disaster, the percentage of simultaneous remote workers can be much higher.
- **VoIP for remote voice services:** Cisco IP Communicator software must be installed on employee desktops. Cisco Unified CallManager must be installed on the network to provide call control to Cisco IP Communicator endpoints. If a Cisco VoIP solution is already installed, providing teleworking voice services is just a matter of deploying Cisco IP Communicator on employee PCs and installing appropriate Cisco Unified Call Manager software licenses.

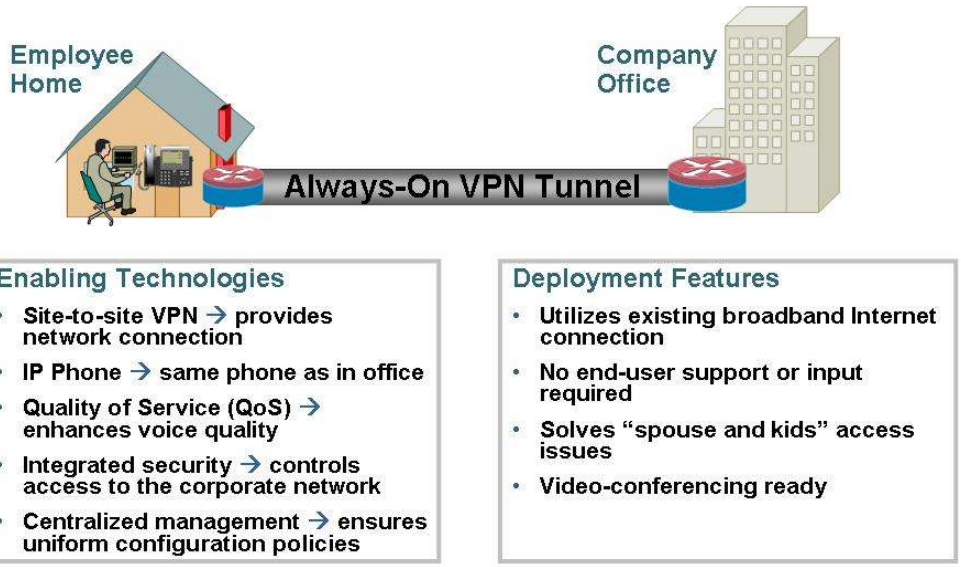
A list of associated Cisco part numbers is available at the end of this data sheet in Table 1.

Cisco Enterprise Class Teleworker: Complete Office Replication

The Cisco Enterprise Class Teleworker enables full replication of the office environment at a fixed location, such as an employee's home (Figure 4). This solution provides superior, toll-quality voice services as well as the capacity for video services (video conferencing, for example). Based on the Cisco Service-Oriented Network Architecture (SONA) framework, the Cisco Enterprise Class Teleworker architecture allows businesses to extend corporate applications to remote employees, enabling them to work more productively and communicate more effectively.

The Cisco Enterprise Class Teleworker solution provides employees with an always-on, secure, and centrally managed connection to the corporate network. This is achieved with a high-speed VPN connection between the teleworker and the headquarters network with a single, highly integrated device behind the broadband (cable or DSL) modem in the teleworker's home. Cisco Enterprise Class Teleworker can use an existing shared home broadband connection.

Figure 4. Cisco Enterprise Class Teleworker Provides Superior, Toll-Quality Voice and Data Connectivity



VPN Connectivity For The Cisco Enterprise Class Teleworker

The Cisco Enterprise Class Teleworker solution uses the same site-to-site VPN technology deployed to interconnect company office sites, but scales it for the individual employee working at home. Cisco site-to-site VPN technology is backbone of the Enterprise Class Teleworker, which uses Cisco Voice and Video Enabled VPN (V3PN) technology to make the teleworker's home a transparent extension of the enterprise.

A Cisco Enterprise Class Teleworker connection supports multiple devices using a VPN tunnel from the home to the corporate office. The teleworker environment supports equipment that includes the enterprise user laptop, home PCs accessing the Internet, and, optionally, an IP phone. A VPN connection is "always-on" and transparent to end users and applications. It does not require the teleworker to use a software VPN client.

When extending rich, always-on data, voice, and video services to the teleworker, there are several factors to consider:

- Ensuring toll-quality voice communications
- Preventing unauthorized persons from accessing the company network when using a shared broadband connection in the employee's home (aka "the spouse and kids problem")
- Securing data and protecting against network security threats across the VPN connection
- Minimizing provisioning and management processes; no dependence on end users for configuration and management
- Providing scalability, performance, and resiliency to dependably connect remote users and provide consistent "in-office" application response times

Cisco Enterprise Class Teleworker integrates security, quality of service (QoS), scalability, and "touchless" provisioning to ensure high communications quality, network integrity, and solution availability.

QoS For The Enterprise Class Teleworker

QoS is a critical component of the Cisco Enterprise Class Teleworker solution. Due to the lower uplink speeds of most residential broadband circuits, upstream traffic can be delayed. This may

affect the performance of mission-critical data and applications that are susceptible to packet delay, jitter, and packet loss, such as voice services. Application performance may also be affected by other activity on the home network, such as a scheduled backup or download. QoS provides consistently acceptable quality for mission-critical data and for delay-sensitive applications. It also provides the ability to create rules for the distinct handling of different traffic types. For example, if a spouse or child is sharing the connection with the teleworker, enterprise traffic can be prioritized, helping ensure high-quality, consistent application performance in support of productivity requirements.

Securing The Enterprise Class Teleworker

Security and user authentication is a critical component of the Cisco Enterprise Class Teleworker solution. Security is integrated completely with all other functions, allowing teleworkers to increase productivity by using networking technology safely and securely. Cisco is the only company that takes an integrated approach to security for all aspects of the network and endpoints. This approach provides the three critical requirements for teleworker security productivity:

- Collaboration between security services and network services—Security is enhanced when network services such as QoS work transparently with IP services. Cisco's integrated approach to security allows for tight collaboration between network technologies and security technologies.
- Complete security features integrated in the teleworker router—Integrated Cisco IOS® Firewall, IPS, time-based access control, and one-touch security configuration lockdown significantly reduce the risk of a security breach, network misuse, and malware proliferation. Identity-based network services (IBNS) provide strong encryption and authentication of both users and devices, helping to prevent attacks by unauthorized users. Using 802.1x, these authentication features can also be used to exclude unwanted devices from the network, or to intelligently route traffic from non-corporate devices directly to the Internet, thus excluding access to the corporate VPN tunnel and resources.
- Comprehensive solution security coverage—Cisco allows you to deploy security everywhere on the network, from PCs and servers to LANs, MANs, WANs, branch offices, and home offices. This provides a homogenous defense system necessary to protect all your most vital processes from threats, both internal and external.

Managing The Cisco Enterprise Class Teleworker

A network that properly supports teleworkers must be capable of verifying, managing, and optimizing user connections to an organization's network. The Cisco Enterprise Class Teleworker architecture enables IT managers to remotely perform day-to-day monitoring and management tasks for devices in the home office. Security and policy management can be performed locally at the home office, or centrally from the corporate headquarters. At headquarters, a corporate IT department has full visibility of remote user sites. IT can apply instant one-to-many configuration and security policy updates (including firewall updates and intrusion detection signatures) without having to wait for the user. Detailed management is possible with tools such as the Cisco IP Solution Center or Cisco Security Manager, which provide scalable monitoring, alerting, and reporting functions for teleworker devices. With tools such as Cisco Service Assurance Agent, IT staff can periodically test the teleworker connection through the VPN and back to the corporate office to view latency, jitter, and packet loss levels at any time. If an end user is experiencing service-level issues, it is possible to monitor the connection and ascertain whether it is an issue

with the service provider or with the teleworking service itself. For enterprise-based VPNs, the management of VPN-related devices can also be outsourced to a service provider.

Cisco Enterprise Class Teleworker Components

Deploying the Cisco Anywhere Office solution requires the following components:

- **VPN for data connectivity:** Cisco 800 Series router at the employee premise. VPN gateway such as a Cisco router or ASA 5500 Series at the central termination location. If a Cisco site-to-site VPN gateway is already installed, only employee premises routers are required (assuming adequate central gateway capacity is available). If desired, WLAN services are available at the employee premises using the Cisco 800 Series router.
- **VoIP for remote voice services:** Cisco Unified IP Phones at the employee premises. Cisco Unified CallManager must be installed on the network to provide call control to Cisco Unified IP Phones. If a Cisco VoIP solution is already installed, providing teleworking voice services is just a matter of deploying IP phones at the employee premises (assuming adequate Cisco Unified CallManager capacity is available).

A list of associated Cisco part numbers is available at the end of this data sheet in Table 2.

Ordering Information

Table 1. Part Numbers for Cisco Anywhere Office

Description	Part Number
Cisco ASA 5500 Series SSL/IPsec VPN Edition (Note: either an adaptive security appliance or router is required, not both)	ASA55xx-SSLxx-K9
Cisco 1800, 2800, 3800, or 7200 Series router (note: either an adaptive security appliance or router is required, not both)	Various
Cisco IP Communicator Software	SW-IPCOMM-E1
Station User License for Cisco Unified CallManager (if not previously installed)	SW-CCM-UL-IPCOMM-E
Cisco Unified CallManager (if not previously installed)	Various

Table 2. Part Numbers for Cisco Enterprise Class Teleworker

Description	Part Number
Cisco 850 or 870 Series router	CISCO85x-K9 -or- CISCO87x-SEC-K9
Cisco 1800, 2800, 3800, or 7200 Series router (if not previously installed)	Various

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 C78-383606-00 12/06