

## BUSINESS READY TELEWORKER

This Q&A is divided into four sections:

- General
- Advance Security and Identity Services
- Advanced Applications
- Management and Support
- References and Case Studies

### GENERAL

**Q.** What is the Cisco® Business Ready Teleworker solution?

**A.** The Cisco Business Ready Teleworker solution is an always-on, secure, and centrally managed connection from a user's home into the corporate network. This solution delivers the full suite of office applications, including IP voice and video, to the user's home office over a broadband connection.

**Q.** What is the business case for teleworking?

**A.** Every year in the United States, businesses lose billions of dollars in lost revenue due to weather shutdowns and other disruptions. The Cisco Business Ready Teleworker solution provides the means to allow work to continue when your workers can not get to the corporate office. The ability to have workers remain productive during bad weather, school holidays, or other events that keep people away from the office but otherwise able to work pays for the solution in less than a year.

**Q.** My employees use software VPN clients to work form home. Why do I need anything more?

**A.** Software VPN clients are fine for checking e-mail, but they do not deliver the full suite of applications that knowledge workers use and depend on every day. In addition, there is simply no way to prioritize or differentiate between different types of home or corporate traffic, which means that voice and video are not practical.

**Q.** If software clients are not the answer, can I have my teleworkers buy a home network switch with a firewall?

**A.** Most “do-it-yourself” (DIY) off-the-shelf VPN devices have the same issues as software VPN clients when it comes to traffic prioritization. In addition, security is left to the individual-leaving the enterprise network exposed to network attacks and viruses. DIY solutions also tend to drive up IT support costs as users typically call the IT staff for advice and help on issues (even when the gear is not officially supported).

**Q.** Can I run The Cisco Business Ready Teleworker solution over dialup?

**A.** Dial speeds are not sufficient for the Cisco Business Ready Teleworker solution; however, residential cable and digital subscriber line (DSL) service work well for high-bandwidth applications.

**Q.** Will the Cisco Business Ready Teleworker solution increase my support costs?

**A.** IT support cost will tend to rise during the rollout phase. However, your IT staff will be able to see, manage, and configure all Cisco Business Ready Teleworker solution routers from a central location, which will likely decrease your support costs for teleworkers and provide much tighter security across your network.

**Q.** Will other Internet users in the home have access during working hours?

**A.** There are several options available, depending on specific enterprise policies. The most common solution uses “split tunneling” (detailed below), which routes noncorporate traffic directly to the Internet service provider's Internet connection and routes corporate traffic back to the enterprise over a secure VPN tunnel.

**Q.** What if my network policies or profiles change? Do all of the teleworkers have to bring their equipment back to the office?

**A.** No. The management solutions available with the Cisco Business Ready Teleworker solution allow your IT staff to remotely configure and apply security updates in a one-to-many “push” to all teleworker routers from a central location-and this is all transparent to the end user.

**Q.** How can I prevent teleworkers from connecting unsecured wireless devices to the network?

**A.** There are authentication solutions on the Cisco Business Ready Teleworker solution routers that can prevent “rogue” devices (such as unauthorized wireless connections) from being connected to the network. Authentication options are discussed below.

**Q.** I don't have IP telephony yet. So why should I deploy the Cisco Business Ready Teleworker solution?

**A.** While IP telephony provides a clear benefit to teleworkers, the advantages of the Cisco Business Ready Teleworker solution include:

- Business resilience and continuance-Continuity of operations with an always-on, secure, IT managed connection to the enterprise.
- Security and manageability-Improved security posture with IP Security (IPSec) Triple Data Encryption Standard (3DES) encryption for all traffic, and security and policy management performed centrally by corporate IT. You do not have to rely on the end user to log on and maintain your security posture, and you get “day zero” protection against viruses and hackers.
- Cost containment and reduction-Consistent and reliable performance for mission-critical and real-time applications over a common network connection, with distinct handling of different traffic types (home vs. corporate users).

In some cases, it is also possible to deploy IP telephony for teleworkers with a system that links back into a key system or private branch exchange (PBX).

**Q.** How can I be sure that my employees who work from home will actually be working?

**A.** While you may not be able to look out the office window to ensure that workers are at their desks, several studies have shown that worker productivity actually increases. Even if productivity remains at a constant rate, teleworkers typically gain time each day due to lack of having to commute. In addition, there many situations where employees must be at their home (due to home repairs or sick children, for example), but could otherwise continue to work. With the Cisco Business Ready Teleworker solution, employees can continue to be productive in these situations.

Cisco also provides tools to monitor the level and performance of traffic over the network connection.

## ADVANCED SECURITY AND IDENTITY SERVICES

**Q.** We need to restrict personal assets from accessing the enterprise network. For example, we want to restrict users that may have a wireless access point or personal computer from accessing the enterprise network. Is there an option that can be configured on the Cisco 830 Series router to restrict or redirect these devices?

- A.** The per-user authentication options include:
- Per-user authentication (Authentication Proxy)
  - 802.1X authentication

You also have VPN device authentication to allow enterprise data access.

IP telephony traffic can be allowed by source or destination access lists. Spouse and child traffic and teleworker Internet traffic can be allowed through the enterprise to the Internet or can be split tunneled.

**Q.** What is Authentication Proxy, and how does it work?

**A.** The Cisco 830 Series router has an integrated firewall that provides an Authentication Proxy function. Authentication proxy requires users to authenticate with the local firewall, which can be customized to provide for different network access per user, based on RADIUS server user definitions. Authentication Proxy can also be customized to require authentication only for access to specific sites, or from specific devices.

When someone tries to gain access to anything (the Internet, for example) behind the Cisco 830 Series router, the person is first prompted for login credentials via a Web interface. These credentials are sent to an authentication, authorization, and accounting (AAA) server, where a decision is made to:

- Send traffic to the corporate VPN tunnel, or
- Send straight out to Internet

**Q.** What are the options for sharing a broadband connection between corporate and home users?

- A.** There are three options:
- Allow sharing with logical split tunneling.
  - Allow sharing with physical split tunneling.
  - Do not allow sharing.

Split tunneling allows traffic that is not part of enterprise communications to go directly to the Internet without being encrypted.

**Q.** What is 802.1X, and how does it work?

**A.** 802.1X provides port-based access control using authentication. Using the 802.1X protocol with Cisco enhancements, the network grants privileges based on logon information.

Only authenticated clients or devices are allowed to connect to the trusted network (enterprise VPN tunnel). Unauthenticated devices will be sent directly to an untrusted network (Internet). You are unauthenticated if:

- You fail 802.1X authentication
- No 802.1X authentication is attempted

Also, 802.1X allows you to apply policies (QoS, VLAN membership, of filters) based on authentication. For example, with 802.1X, you can set up two different Dynamic Host Control Protocol (DHCP) pools. You can assign addresses in a network 10.0.0.0 address space to devices that can authenticate properly. For a device that doesn't offer the right credentials, you can assign them to a network 192.0.0.0 address space dynamically. The device can then be used to determine the traffic that is permitted or not permitted in the tunnel. You can differentiate and allocate multiple DHCP pools on the Cisco 830 Series router.

**Q.** My organization doesn't currently support an OS with an 802.1X supplicant. What are my options for restricting assets from accessing the enterprise network?

**A.** Your options are Authentication Proxy and access control lists (ACLs).

**Q.** How does the Cisco 830 Series Router identify a Cisco IP phone if there is no 802.1X supplicant on the phone?

**A.** 802.1X differentiates between authorized and unauthorized access points via a supplicant on the device. Today, the Cisco 830 Series router identifies a Cisco IP phone with Cisco Discovery Protocol, and permits access. In the future, an 802.1X supplicant on the IP phone will authenticate with corporate digital certificates in the same way as a corporate laptop.

**Q.** Can we transparently send all teleworker traffic to the enterprise VPN tunnel, and redirect all personal traffic from the home network directly to the Internet?

**A.** Yes. PCs behind the Cisco 830 Series router can have Internet access through the VPN tunnel provided by the enterprise, or directly to the Internet, using split tunneling:

- Teleworker PC: Internet access through enterprise
- Home PCs: Split tunnel directly to the Internet

The option chosen depends on the enterprise security policy. Split tunneling is efficient because it encrypts only business-related traffic and avoids sending Internet traffic in and out of the enterprise network.

**Q.** If the enterprise is paying for an employee's broadband service at home, then we don't want personal users behind the Cisco 830 Series router. How can we still accommodate the “spouse and kids” using the same broadband connection to the Internet?

**A.** Use physical split/user-based tunneling. For example, insert a Linksys device between the broadband modem and the Cisco 830 Series router. Then attach your home network to the Linksys device.

**Q.** What are the implications of using physical split tunneling? What happens if you place a Linksys device between the Cisco 830 Series router and the broadband modem?

**A.** The risk with this approach is that while you are locking security down more tightly behind the Cisco 830 Series router, you may introduce a risk to voice quality. Linksys currently has no integrated quality of service (QoS), so home network traffic may interfere with corporate upstream traffic. The Cisco 830 Series router contends with the spouse and children PCs, as the Linksys does not prioritize the teleworker traffic.

Again, this depends on your uplink speed. The recommendation is that the Cisco 830 Series router is the first device behind the broadband modem if you are using IP telephony (voice).

**Q.** Does the Cisco Business Ready Teleworker solution provide firewall, intrusion detection, and URL filtering?

**A.** Yes. All of these functions are integrated in the Cisco 830 Series router.

## ADVANCED APPLICATIONS

**Q.** Why do I need QoS?

**A.** Throwing more bandwidth at delay-sensitive and bandwidth-intensive applications such as streaming video, voice, and other mission-critical services is costly, and may not be enough in the long term to ensure the level of service required. The most viable economical solution is a QoS network, including IP QoS support in the core and edge that results in significantly decreased capital and operational expenses (as well as well-served, satisfied customers).

End-to-end, standards-based QoS provides secure, predictable, and measurable services to these applications by managing delay, delay variation (jitter), bandwidth, and packet loss in a network.

**Note:** There is a mismatch between Ethernet speeds to the broadband modem, and a much lower uplink speed to the broadband network. Accordingly, it is necessary to prioritize and shape traffic to the uplink speed. This is the most important component for voice quality and real-time applications—the ability to prioritize traffic before it arrives at the broadband modem.

**Q.** What are the benefits of deploying IP telephony over the Cisco Business Ready Teleworker solution?

**A.** With the Cisco Business Ready Teleworker solution, you no longer tie up a home phone line, and “on-net” calls are free with toll bypass. In Cisco's pilot of the solution, the company saw a cost savings of \$100 per month in phone charges per employee.

**Q.** We would like to prioritize teleworker traffic over other home-user traffic. Is there an option that can be configured on the Cisco 830 Series router to identify and differentiate traffic types?

**A.** Yes. Cisco QoS.

**Q.** Can we use an IP softphone in lieu of an IP phone?

**A.** Yes. A Cisco IP SoftPhone can be used with IP telephony over the Cisco Business Ready Teleworker solution.

**Q.** We don't have IP telephony in our enterprise. Can we achieve “same number reachability” for teleworkers with our legacy PBX systems?

**A.** Yes. Internetworking with some legacy PBX systems may be possible, depending on the vendor and features it supports.

**Q.** Does the IP phone take up one of the ports on the Cisco 830 Series router?

**A.** Yes. But you have a port on the back of the IP phone where you can plug in a laptop; it acts as a switch, so you can recoup a port. The Cisco 830 Series router currently does not have inline power, so you need a power supply for the phone.

**Q.** Does the IP phone stay on all the time?

**A.** Yes. The Cisco 830 Series router is authenticated all the time to your central site as an always on VPN tunnel. As long as that phone is plugged into the router, it will be registered and always on. IP telephony traffic traversing the IPSec VPN is transparent to all users and personnel managing the IP telephony network.

**Q.** Does the Cisco 830 Series router have dial backup?

**A.** Yes. Out-of-band dial backup is a feature on the Cisco 830 Series router. However, you have to connect to a dial modem.

**Q.** Cisco's internal Business Ready Teleworker solution pilot results show that voice quality is 96 to 98 percent high quality. What does this measurement mean?

**A.** In Cisco's pilot trials, 96 to 98 percent of people reported that their calls were of high quality. The two to four percent was most often attributable to either not following design rules or to a broadband network outage issue.

**Q.** Is there a recommended minimum speed to deploy IP telephony? Does Cisco recommend a minimum bandwidth for the Cisco Business Ready Teleworker solution?

**A.** On DSL there is more overhead, so Cisco recommends a minimum uplink speed of 160 Kbps, and 256 Kbps for predictable voice quality. When you get down to the 128-Kbps uplink speed range, the quality varies, depending on the service provider. Good quality is possible, but you want repeatable performance from service provider to service provider. In these cases you will need to do some investigation to see what kind of upstream bandwidth you can get. Testing shows that 256 Kbps upstream provides consistent voice quality. The general guidelines are that more bandwidth is better, and that asymmetric speeds are preferable.

**Note:** Cisco recommends provisioning G.729 codecs for IP telephony calls across the WAN (public Internet) for the Cisco Business Ready Teleworker solution.

**Q.** How can I tell what the upstream and downstream speeds of my service provider are?

**A.** There are several standard online tests to measure the broadband speed you are getting, both up and down. For example: <http://www.broadbandreports.com/stest>

**Q.** Why can't I use a Cisco PIX® 50X Series router in the teleworker home office?

**A.** The Cisco PIX 50X can be an excellent home-office device. While these products are very fast, they cannot prioritize traffic (no integrated QoS). While voice quality may sound fine with no other traffic, as soon as you plug in a laptop and use data or download a large file, the quality of voice or real-time applications may degrade. Data starves such traffic at the broadband modem.

If you turn on integrated QoS on the Cisco 830 Series router, you can achieve high quality for voice and real-time applications.

**Q.** I understand that QoS will work in the VPN tunnel. But once you get to a service provider network, performance is “best-effort.” How does congestion in a service provider “best-effort” network affect application performance with the Cisco Business Ready Teleworker solution?

**A.** In live trials, we have not seen an issue with contention on either DSL or cable broadband networks-both services work well. Again, it depends on your service provider.

**Q.** If you encrypt voice, does that introduce delay that may affect voice quality?

**A.** Cisco hardware encryption adds minimal delay, and the Cisco 830 Series router has built-in hardware encryption.

**Q.** Do I need a premium broadband service?

**A.** It depends. You should investigate the broadband residential circuit options available and pilot those options before selection. Have realistic expectations about voice quality over best-effort service provider networks if the service provider does not provide QoS. Choose a provider offering QoS service-level agreements (SLAs), or if not available, the most capable best-effort provider (least delay, most bandwidth, greatest availability and coverage).

## MANAGEMENT AND SUPPORT

**Q.** We would like to deploy numerous home-office VPN routers. As we add each new home router, how can we authenticate individual devices?

**A.** There are multiple options that can be used-separately or together-to provide authentication for network devices (i.e. the Cisco 830 Series router) in teleworker sites:

- Shared secrets with a RADIUS server back end provide scalable authentication
- Digital certificates allow for highly secure and scalable authentication
- Easy VPN provides for simplified scalability by simple definitions and preset combination of authentication options

**Q.** Can I push policies and manage devices over the same VPN connection?

**A.** Yes. You can push configurations out and apply authentication and security policies over the access connection and VPN tunnel. Several network management and monitoring tools are available, including the Cisco IP Solutions Center (ISC), Simple Network Management Protocol (SNMP), and Cisco NetFlow.

## REFERENCES AND CASE STUDIES

**Q.** Is Cisco using the Business Ready Teleworker solution?

**A.** Yes. Cisco has deployed a pilot Business Ready Teleworker solution. Currently, approximately 600 U.S. employees with residential-class cable and DSL broadband access services have the solution in their homes (Cisco 830 Series routers with VPN, and Cisco IP Phone 7960 systems). The pilot has been very successful, and Cisco is continuing to add users across the company. The technology works and we understand how it scales; now our focus is on putting policies in place to support the process-getting users the hardware, manager approval, and so on.

**Q.** Where can we go for more detail on how to design and deploy this solution?

**A.** For more information, the Teleworker Design Guide is available at: [www.cisco.com/go/srnd](http://www.cisco.com/go/srnd)



**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](http://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

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website 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. (0402R)