

# Secure Managed VPN Services for Cable Operators

## Cisco® Solutions for Delivering Secure Video, Voice, and Data Services to Commercial Customers

Cable operators understand that to grow revenue you have to look beyond the traditional cable television and data services delivered to residential subscribers. It means offering new types of services to new types of customers, including the highly attractive market of small/medium businesses (SMBs). These commercial services go beyond broadband Internet access over a cable modem, instead delivering secure virtual private networks (VPNs).

Traditionally, VPNs have been used only for data communications. Today, many businesses want to converge all communications—video, voice, and data—onto a single network. These commercial customers also expect support for converged communications across VPNs to enable greater efficiency and cost savings. Cable operators can meet this expectation—and gain new customers, new revenue, and a competitive advantage—by offering secure managed VPN services.

Cisco Systems® is meeting business requirements for convergence with solutions for delivering voice and video as well as data over a VPN that is based on the IP Security (IPSec) protocol. These solutions will enable cable operators to offer managed VPN services to commercial customers over an IP backbone without compromising communications quality, security, or reliability. Cable operators can deliver these services over current coaxial or hybrid fiber-coaxial (HFC) networks and network equipment that is compliant with DOCSIS.

## What Are Secure Managed VPN Services?

From a customer's perspective, VPNs offer a low-cost and highly flexible alternative to dedicated, private networks based on telephone company DS0, fractional T1, T1, ISDN Basic Rate Interface (BRI), Frame Relay, or ATM services. VPNs use a shared network, such as a cable operator's backbone, with user sessions carried over separate, encrypted tunnels within that network to ensure privacy and security. The cable operator (or a selected system integrator) manages the service and associated customer premises equipment (CPE)—such as routers and firewalls—enabling a business to fully outsource its communications.

For commercial customers, the key benefits of managed VPN services include:

### Reduced Costs

A managed VPN service provides a lower-cost alternative to a private network while continuing to meet stringent performance and security requirements.

### Integrated Communications to Remote Locations

Businesses can reduce expenses for equipment, access lines, and toll charges by integrating video, voice, and data on the VPN. Remote offices and telecommuters can connect to a corporate private branch exchange (PBX) and internal video broadcasts as well as to data applications.

## **Support for Advanced Applications and Communication Technologies**

A multiservice VPN supports multimedia applications that take advantage of the latest technologies in IP telephony and IP video.

### **Outsourcing advantages**

SMBs typically do not have the resources and cannot afford to maintain their own networks. These businesses have a propensity to buy managed service offerings from a provider such as a cable operator. For a cable operator, a managed VPN service presents several benefits, including:

- A means to attract new commercial customers and generate ongoing revenue from monthly service fees
- Opportunity to sell these customers additional services as they become available
- Ability to take advantage of investments in a broadband network infrastructure because a VPN service is a simple service overlay
- Compatibility of IPSec VPNs with a future upgrade of the network backbone to Multiprotocol Label Switching (MPLS)

### **Market Opportunity**

Secure managed VPN services offer cable operators the appeal of a rapidly growing commercial market. The market research firm IDC expects the VPN market in the United States to grow from \$2 billion in 2002 to over \$5 billion in 2006. By 2006, remote-access VPNs are expected to account for \$3.7 billion of that forecast while site-to-site VPNs account for the remaining \$1.3 billion.

Within the commercial market, SMBs represent the most attractive target for selling managed VPN services. Small/medium businesses (100 to 1000 employees) want VPNs to deliver increased bandwidth for remote users and the ability to add new users quickly. Security, quality, and flexibility are also important criteria for small/medium businesses in choosing VPN services.

Small businesses (20 to 100 employees) are extremely price-sensitive, they are interested in outsourcing because they often lack in-house expertise, and they prefer bundled solutions. Outsourced VPN services for these businesses must be able to offer reduced costs and simple connection of remote sites and users.

Cable operators can also look at vertical industries as a way to identify potential customers. These industries include local or regional retail, small manufacturing, legal and professional firms, education, local government, health care, and financial institutions. Applications that can be carried over VPNs include e-commerce, distance learning, videoconferencing, off-site extensions for a PBX and voice-mail system, image and file transfers, and supply-chain management.

### **Business Drivers**

The demand for VPNs continues to grow because of market drivers such as the following:

#### **Business Drivers**

Enterprises want to take advantage of VPNs for several reasons, including cost savings compared to traditional networks, the need to create secure intranets and extranets, the challenges of supporting new applications, and the need to focus on core activities.

## Technology Drivers

IP is quickly replacing Frame Relay and ATM as the standard for enterprise networks. Supporting this adoption are advances in key technologies such as IPSec for communications security, Quality of Service (QoS) for distinct handling of different traffic types, and accelerated packet processing for overall network performance.

## User Drivers

SMBs need to securely connect ever-growing numbers of remote sites, mobile users, suppliers, and customers to internal networks. As more users become accustomed to the speed of residential broadband services, they will expect comparable high performance from their corporate network connections.

## Security Drivers

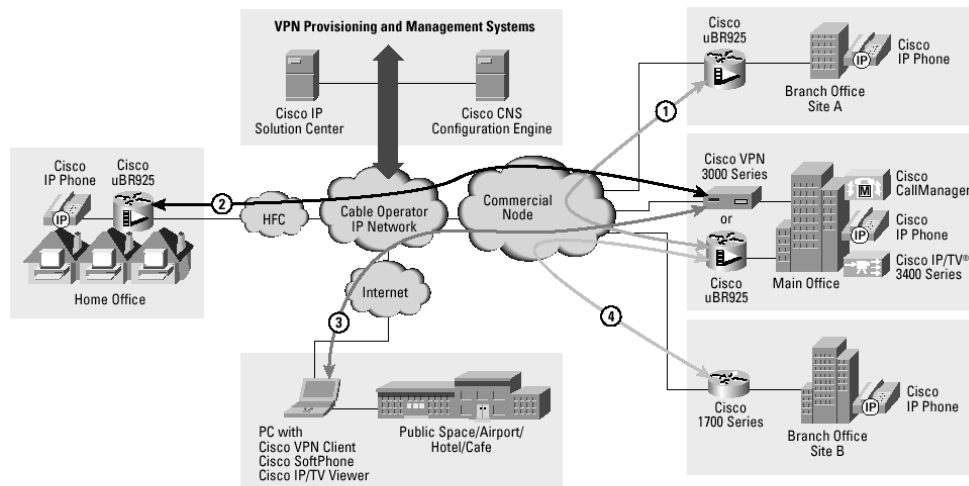
Businesses understand the need to protect their information assets from security breaches and risks. Yet not all businesses have the internal resources necessary to proactively implement, manage, and keep current with the latest security advances.

## Deployment Models

Cisco provides three deployment models for managed VPN services through Cisco AVVID (Architecture for Video, Voice and Integrated Data) for converged networking and the SAFE Blueprint from Cisco. These deployment models correspond to the different connectivity needs of remote-site, telecommuter or teleworker, and mobile users (Figure 1).

**Figure 1**

A Cable Operator's Secure, Managed VPN Service Gives SMBs a Complete Solution for Connecting Remote Sites, Home Offices, and Mobile Users



### Cisco VPN Solutions for Video, Voice and Data Services

- ① Branch Office Site A ↔ Main Office (Site-to-site)
- ② Home Office ↔ Main Office (Telecommuter remote access VPNs)
- ③ Public Space ↔ Main Office (Mobile worker remote access VPNs)
- ④ Branch Office Site B ↔ Main Office (Cisco IOS® Software-based VPN)

## Site-to-Site Deployment Model

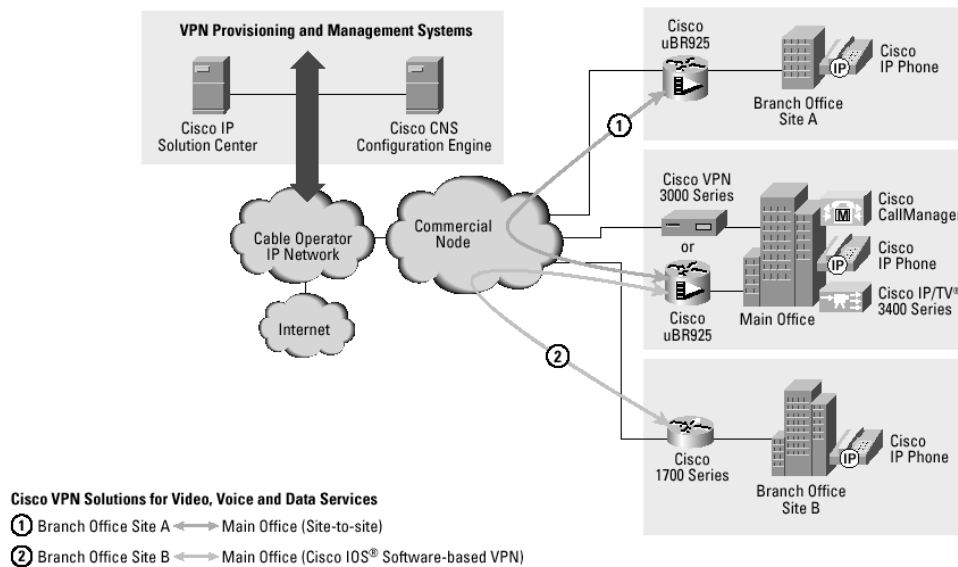
Small/medium businesses typically need network connections for multiple branch offices, retail stores, or other sites within a city or region. The site-to-site deployment model creates IPSec tunnels for user sessions over a cable operator's IP backbone network (Figure 2). It is designed to connect a main office and one or more remote sites and serve multiple users in each remote location. This model provides many of the same capabilities as a traditional private network, with support for both hub-and-spoke and mesh topologies.

In the site-to-site model, a secure, managed VPN service offers the following benefits:

- It connects all sites in a simpler, more efficient, and less-expensive solution than a traditional private network.
- Businesses can take advantage of VPN bandwidth and QoS features to carry internal voice and video traffic on the same VPN, further reducing communications costs.
- A single VPN access link can serve multiple users at each remote site, with a typical access speed of up to 1.5 Mbps.
- Separate, encrypted tunnels for each user session assure communications privacy.
- End-to-end security can be achieved by carrying all VPN traffic exclusively on the cable operator's backbone and access networks.

**Figure 2**

The Site-to-Site Model Offers Secure VPN Connections for Multiple Users at a Remote Site to the Internal Network at a Main Office



## Small Office/Home Office

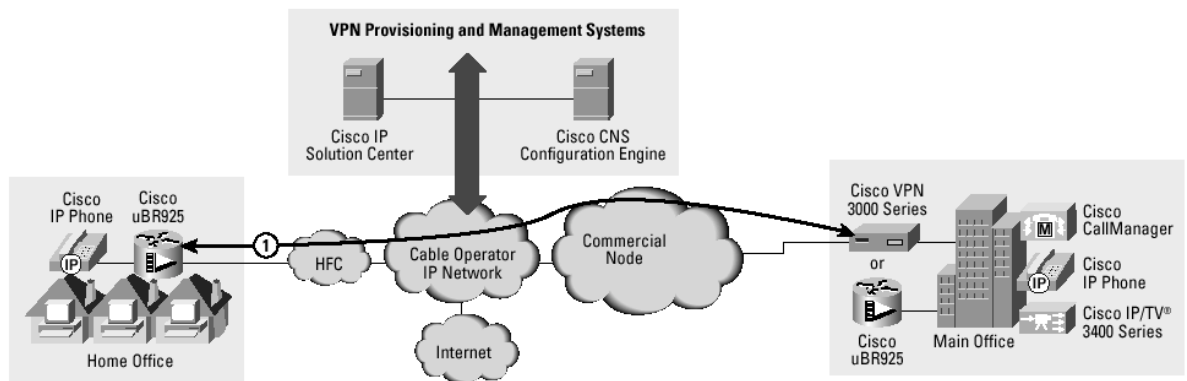
Employees who work at home (telecommuters or teleworkers) need access to all corporate data and applications for improved productivity and business continuity. Designed for connections between a main office and small or home offices, the small office/home office (SOHO) deployment model also creates IPSec tunnels, but may utilize multiple access providers in order to serve users in different areas (Figure 3). This model provides the same capabilities as a traditional hub-and-spoke WAN that connects branch offices and telecommuters.

In the SOHO model, a managed VPN service offers several advantages, such as:

- The VPN connection is “always on,” giving the user instant access to all network services.
- IP telephony technology for voice communications means the telecommuter can preserve the same PBX extension number and voice-mail access as if working at the office. No separate phone line is required for business calls, reducing monthly telephone service and toll charges.
- Support for video on the same network connection enables a user to participate in videoconferences and view streaming-video files.

**Figure 3**

The SOHO Model Gives a Telecommuter Advanced Video, Voice, and Data Services that Are Not Available over a Residential Broadband Internet Connection



**Cisco VPN Solutions for Video, Voice and Data Services**

① Home Office ↔ Main Office (Telecommuter remote access VPNs)

**Remote Access**

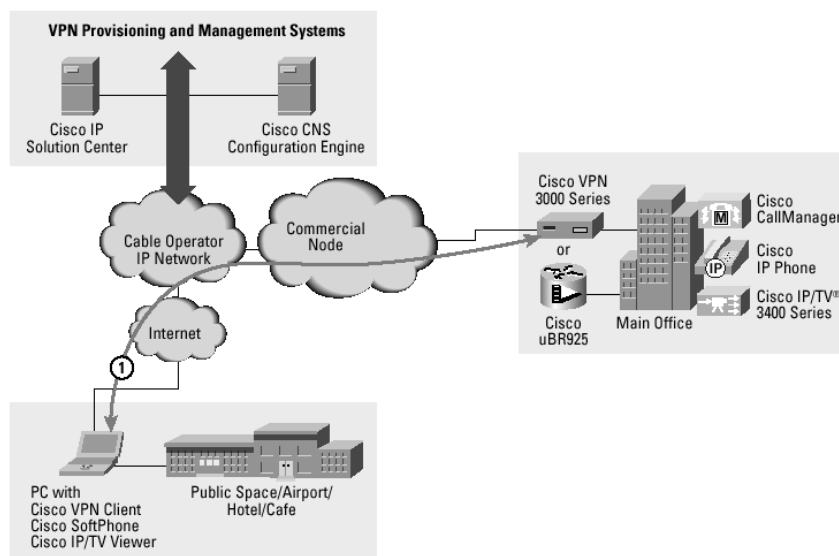
Traveling employees can be more productive if they can gain easy, secure access to the company network from any location. The remote-access deployment model connects a mobile user to a company’s internal network (Figure 4). This deployment model utilizes IPSec tunnels over the networks of multiple providers (backbone and access) and provides the same capabilities as a traditional high-speed service for remote access to an enterprise network.

A managed VPN service can implement this model by providing VPN connectivity over any type of Internet access, including:

- Dialup Internet access points in the cable operator’s service area
- A broadband Internet access service such as those provided in hotels and conference centers
- Wireless “hot-spot” access as a direct service or through agreements with local wireless Internet providers

**Figure 4**

The Cisco Model for a Remote-Access VPN Extends this Commercial Service to a Customer's Mobile Employees



**Cisco VPN Solutions for Video, Voice and Data Services**

① Public Space ↔ Main Office (Mobile worker remote access VPNs)

**Cisco Solutions for Secure Managed VPN Services**

To deliver secure managed VPN services, cable operators need networking and security solutions that are built upon strong architectures and designed to meet the distinct requirements of cable networks. Cisco offers products for all aspects of managed VPN services, including the following:

- On-premises cable modems and routers (CPE) and headend cable modem termination systems (CMTSs)
- VPN routers and access concentrators
- Firewalls, intrusion detection systems, and other security products
- Cisco IOS® Software, with sophisticated features for VPNs and security
- IP call-management systems and IP telephones
- IP streaming-video and live-broadcast systems
- Service provisioning and management applications

Cisco's proven cable products have received DOCSIS 1.0, DOCSIS 1.1, and PacketCable 1.0 qualifications. The DOCSIS 1.1 qualification is important for meeting the expectations of larger businesses for Quality of Service (QoS) and bandwidth guarantees via service-level agreements (SLAs). And in the future, PacketCable compliance will be critical for supporting voice communications on a very large scale within a market area.

**Why Cisco?**

Cisco Systems is uniquely positioned to offer cable operators a wide range of products and solutions for secure managed VPN services to commercial customers. Because Cisco offers end-to-end network solutions, cable operators can enjoy the assured interoperability of converged communications over IPSec VPNs.

Working with Cisco Systems also brings cable operators the following advantages:

- Industry-leading expertise in cable, IP, and security technologies, coupled with a deep understanding of the communications needs of SMBs
- A proven, comprehensive set of solutions for cable commercial services that address market opportunities today and into the future
- The only provider of an end-to-end architecture that enables cable networks to support all service requirements
- Flexible networking solutions that embrace evolving architectures, market needs, and cable standards
- A single source for products, network design guidance, and support

#### For More Information

To learn more about Cisco VPN solutions and other Cisco products and services for cable operators, visit:

<http://www.cisco.com/go/cable>.



**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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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.  
(0304R) RDA4680-04/03