How Cisco IT Uses Network Management Products to Improve Teleworker Solution Scalability

Zero-touch deployment and configuration management create a sustainable global deployment and support model.

Cisco IT Case Study / Network Management / Remote Access Network Management This case study describes Cisco IT's internal deployment of Cisco IP Solution Center and the Cisco CNS Configuration Engine to provide automated provisioning and configuration management of remote devices for remote-access hardware-based VPNs within the Cisco IT network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"Cisco IP Solution Center and the Cisco CNS Configuration Engine have enabled us to achieve a 95-percent success rate for automatically provisioning new Cisco Virtual Office users."

– Kevin R. Kelleher, Systems Administrator, Cisco IT

BACKGROUND

With the introduction of a home-access router-based VPN solution (the Cisco Virtual Office solution, formerly known as Enterprise-Class Teleworker) in August 2004, Cisco Systems® created a complete, fully integrated solution that extends time- and cost-saving corporate resources to Cisco® employees at home. Cisco Virtual Office, as the solution is called within Cisco IT, represents a breakthrough in remote VPN access. With its support for quality of service (QoS) for voice and video, and flexible security options such as device and user authentication, firewall-based protection, and intrusion detection, Cisco Virtual Office brings enterprise-class service, performance, and security to the home office. The solution combines a Cisco router (in early 2006, either the Cisco 831 or 871 Integrated Services Router) with a high-speed broadband Internet connection (usually via DSL or cable), along with Cisco IOS® Software. Cisco Virtual Office provides a secure, encrypted, "always-on" connection that is quick to initiate for the user and easy for Cisco IT to manage.

This document discusses the role of two network management devices, Cisco IP Solution Center and Cisco CNS Configuration Engine, which Cisco IT used to great advantage in automating the complex provisioning and management functions that were required in managing several thousand routers.

CHALLENGES

In rolling out Cisco Virtual Office to thousands of users, Cisco IT recognized two major challenges: provisioning and management. The provisioning process for the solution was labor-intensive. During the initial Cisco Virtual Office trial, a Cisco IT technician had to manually configure each Cisco router before it was sent to the new teleworker. First, the engineer would generate a configuration using the Cisco IP Solution Center appliance—a 13-step process. Then, the engineer would manually copy the configuration onto the new router. This process often took up to two hours per router. "Our best engineer working as fast as possible would configure a router in about 45 minutes," says David Iacobacci, network engineer for Cisco IT who worked on the Cisco Virtual Office project. "There was no way Cisco Virtual Office could scale to allow Cisco—or any company—to add hundreds or thousands of teleworkers."

With the potential for adding thousands of routers to the Cisco network, the prospect of configuring and managing all these new network elements located remotely in peoples' homes loomed large for Cisco IT. Outsourcing the configuration task to another firm would allow Cisco IT to support the service without having to add employees, but

the cost of the service would become prohibitive. It was clear that provisioning and management of Cisco Virtual Office had to be automated.

SOLUTION

Automating the Cisco Virtual Office configuration and deployment process required integrating several technologies, products, and platforms. Two of these, Cisco IP Solution Center and the Cisco CNS Configuration Engine, play a major role in enabling automated provisioning of Cisco Virtual Office routers—referred to as “zero-touch” deployment—and ongoing configuration management of those devices.

Cisco IP Solution Center is a family of intelligent element management applications that help reduce overall administration and management costs by providing automated resource management and rapid profile-based provisioning capabilities that facilitate fast deployment. Cisco IP Solution Center has most commonly been used by service providers for establishing connections between routers at a central site and routers at various client locations. The Cisco CNS Configuration Engine works in conjunction with IP Solution Center, downloading configuration and policy information to remote routers. “If Cisco IP Solution Center and Cisco CNS Configuration Engine hadn’t existed, we would have had to build that knowledge into our own enterprise management system, which would have cost us a lot of time and money,” says Kevin R. Kelleher, systems administrator, Cisco IT Management Services. “And we would have had to automate the entire process at a lower level.”

With Cisco IP Solution Center and the Cisco CNS Configuration Engine, Cisco IT had to build several new functions into its enterprise management system: functions that would automatically set up VPN tunnels and policies and IP security (IPsec) encryption keys, functions that would generate home router Cisco IOS® Software configurations automatically, and functions that would push these configurations from a central point across the Internet to each one of the thousands of routers in different homes around the world.

The Provisioning Process

The role of Cisco IP Solution Center and the Cisco CNS Configuration Engine in Cisco Virtual Office provisioning can be most easily illustrated by following the process, described step-by-step, from initial user request to successful installation.

Initial user request

The user fills out a request for new service using Cisco IT’s web-based service request system. The request is checked by the web-based entitlement system. These systems (part of the Cisco IT enterprise management suite of automated systems) interface via open Extensible Markup Language/Simple Object Access Protocol (XML/SOAP) and the rich API set supported by Cisco IP Solution Center. “The IP Solution Center’s support of XML/SOAP standards and APIs made integrating it with our enterprise management system much easier,” says Kelleher. “The API set on the IP Solution Center is working very well for doing our provisioning. It takes 13 steps to set up the router using the IP Solution Center. We simply use the APIs already available, and have automated each of these 13 steps.”

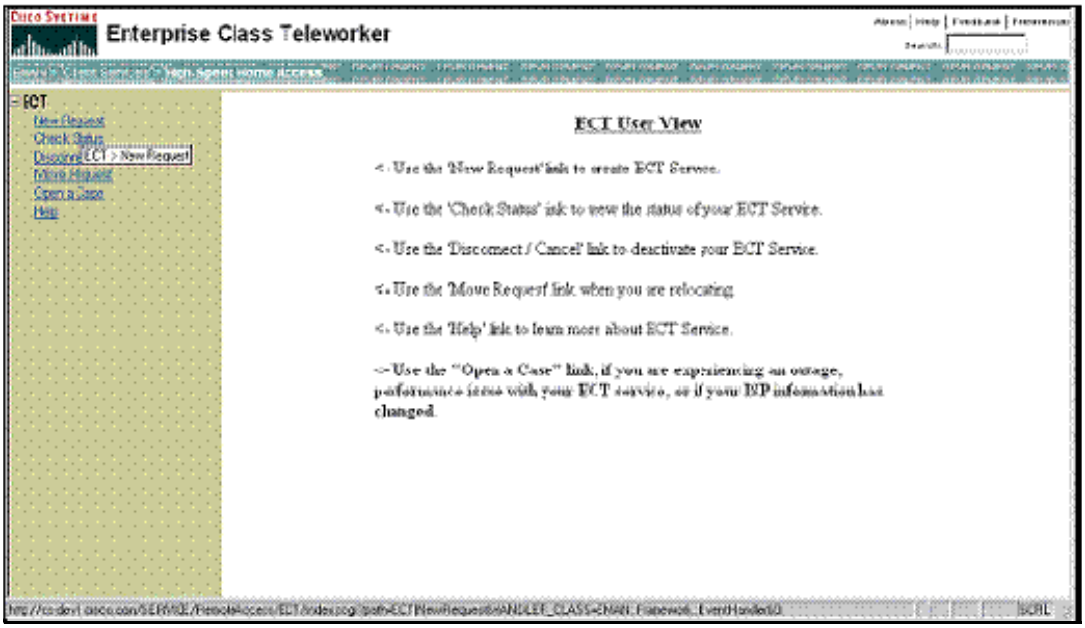
The process begins with the employee filling out the online sign-up form, as shown in the following diagrams.

Cisco Virtual Office Service Request Process

Step 1. Open your browser to the Cisco Virtual Office Service Request website.

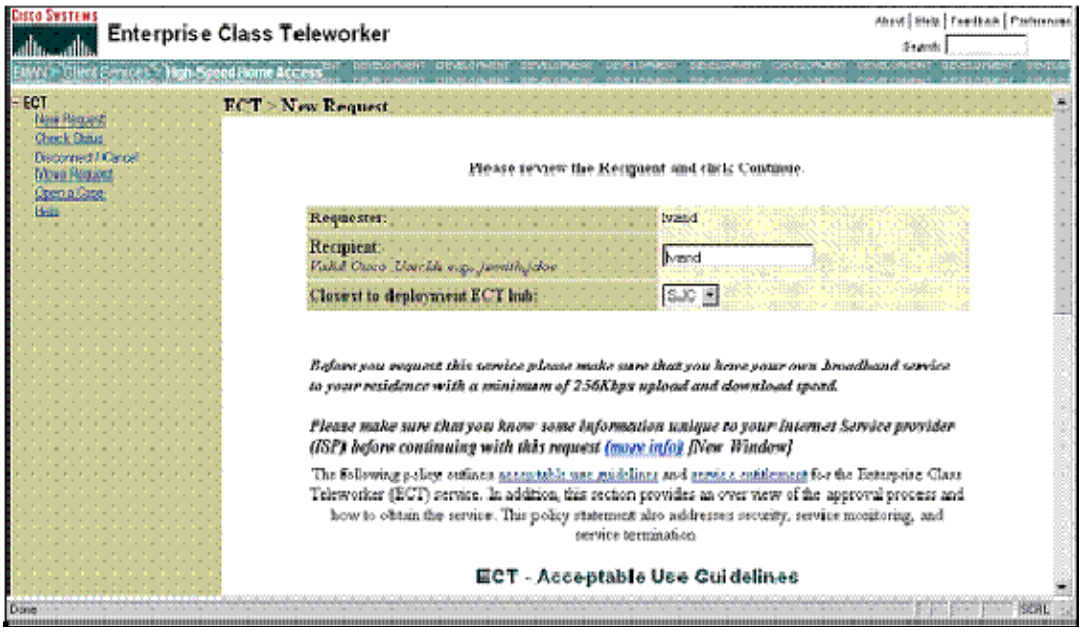
From the left-side menu, click “New Request” (Figure 1). This will begin the Cisco Virtual Office Service Request.

Figure 1. Cisco Virtual Office Service Request Website



Step 2. Enter your Cisco username in the “Recipient” field and select the hub location closest to your residence (Figure 2). Note: By default, these fields will be autopopulated based on your HR information. Be sure to verify this information before proceeding.

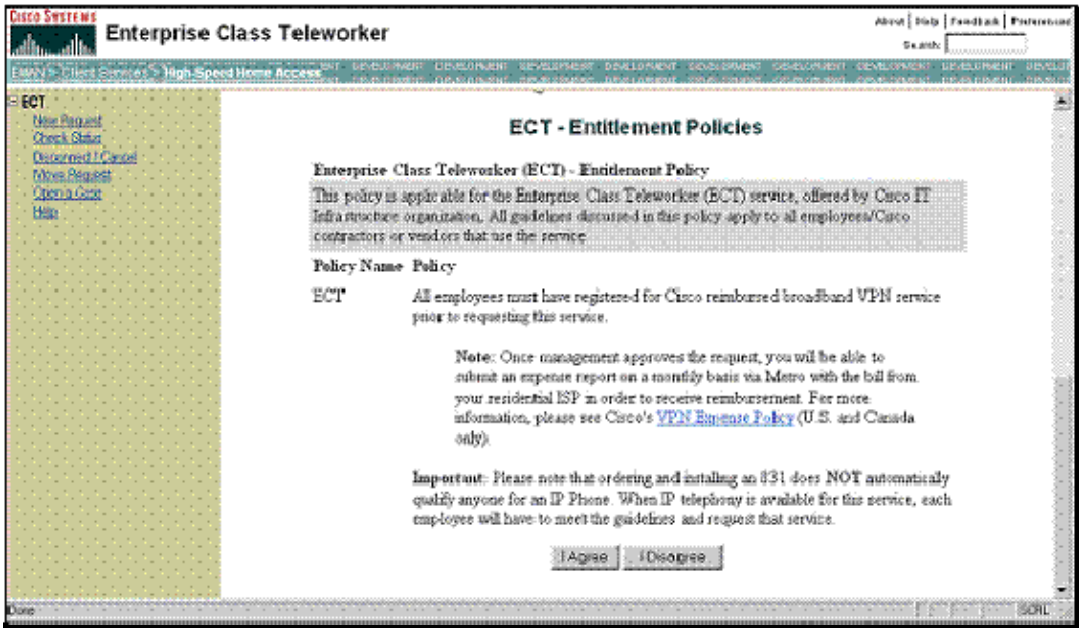
Figure 2. Enter Username and Select Hub



Step 3. After reading the Entitlement Policies, select the appropriate response at the bottom of the page to continue (Figure 3).

If you do not agree or determine you are not eligible, select “I Disagree”. Your service request session will be terminated.

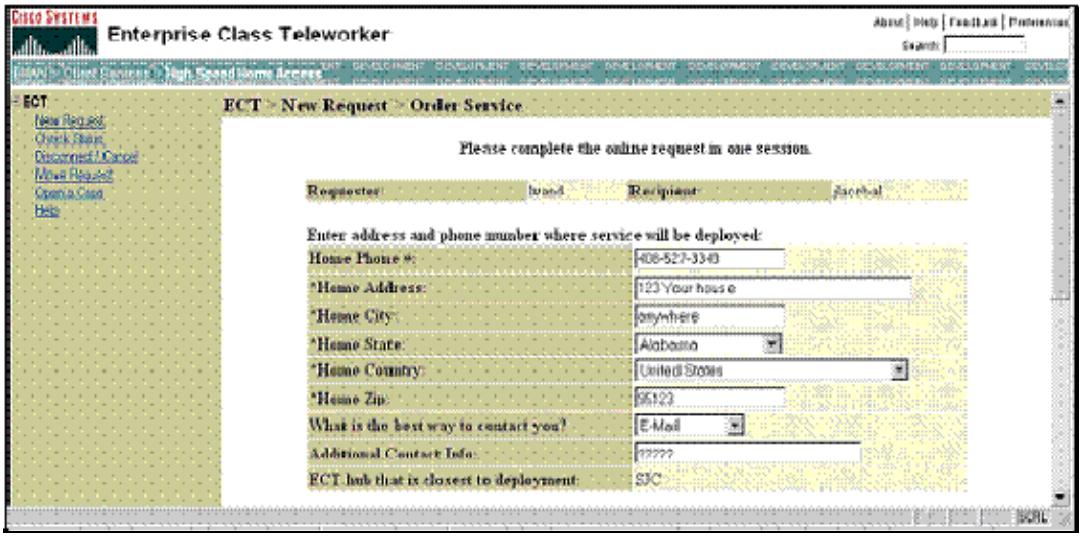
Figure 3. Cisco Virtual Office Entitlement Policies Agreement



By selecting “I Agree”, you agree to comply with the Cisco Virtual Office entitlement policies. Next, you will be directed to complete the Service Request (Figure 4). All required fields are marked with an asterisk (*). Your request will not be processed until complete.

Step 4. The first section of the Service Request gathers your address and contact information. This is not used for any purpose other than to assist with support of your Cisco Virtual Office service.

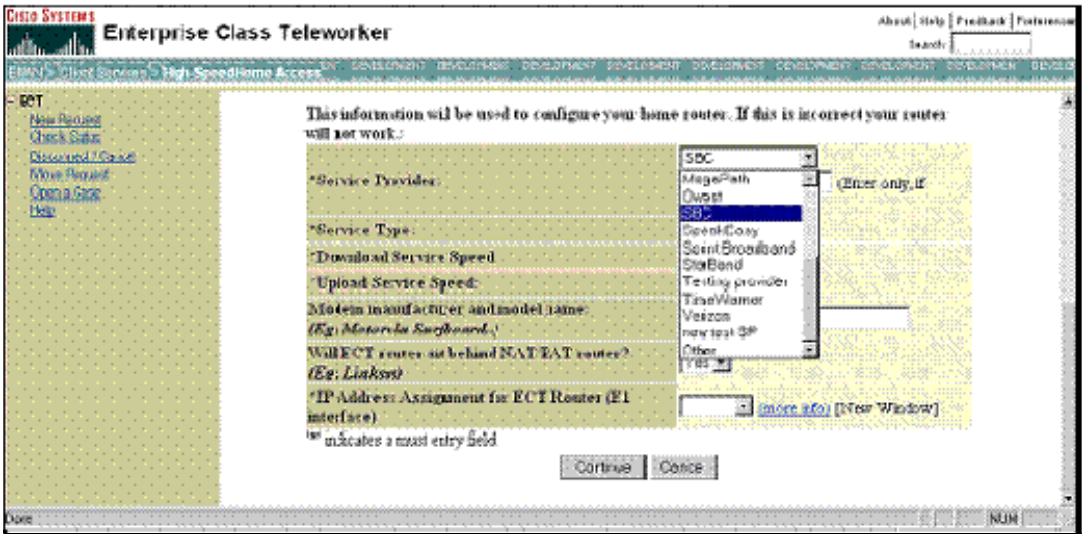
Figure 4. Address and Contact Information



Step 5. The lower section of the page gathers information required to configure your Cisco Virtual Office router. If you are uncertain about any of the required fields, do not complete the request. If these entries are inaccurate, your Cisco Virtual Office configuration may be jeopardized. To exit the Service Request, select “Cancel” at the bottom of the page at any time. Note: Your entries will not be saved.

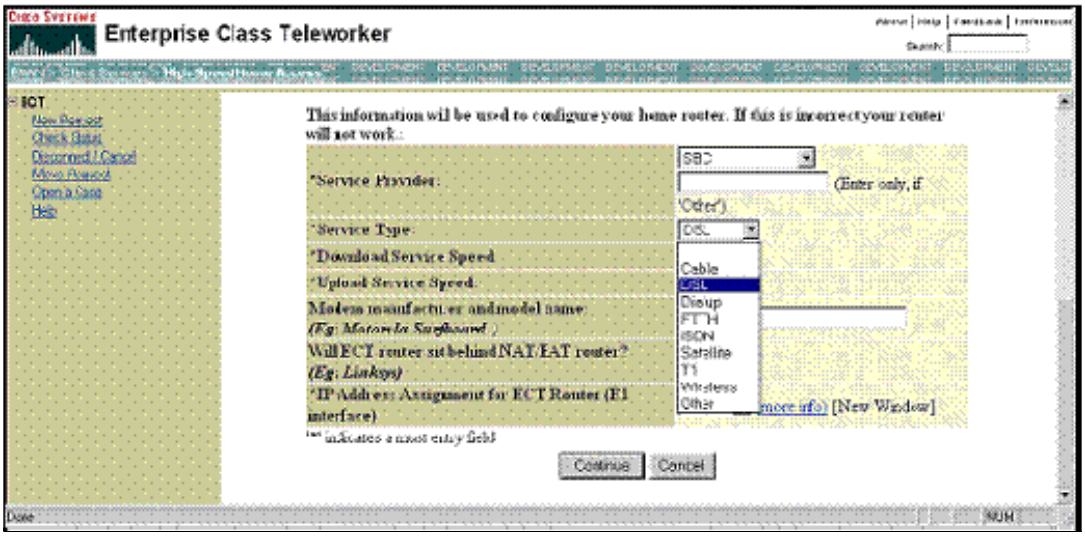
Select your home service provider from the drop-down menu (Figure 5). If your provider is not listed, select “Other” and enter your ISP name in the field provided.

Figure 5. Enter Home Service Provider



Step 6. Select the appropriate ISP service type from the drop-down menu (Figure 6).

Figure 6. Enter ISP Service Type

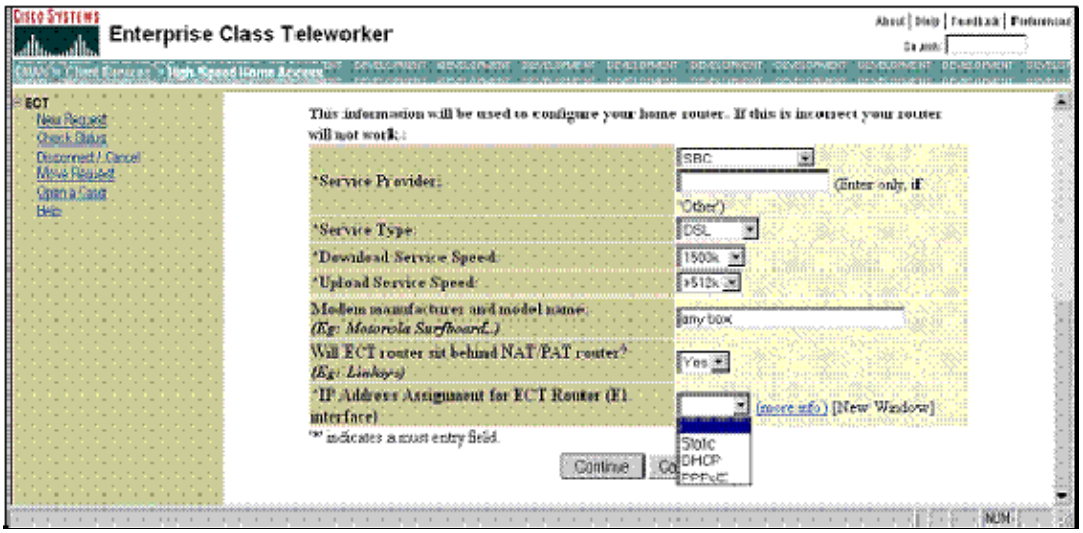


For the download service speed and upload service speed, you must select the best match for your service. Note: If your speed is not listed, select the nearest match that is not greater than your speed.

If the Cisco Virtual Office router will be positioned behind a device that serves Network Address Translation/Port Address Translation (NAT/PAT) into your home network, you must select “Yes” for this question.

Step 7. Next, you will be asked to select the type of E1 interface for your Cisco Virtual Office router's IP address assignment (Figure 7). The "more info" link has been provided to assist you if needed. Your selection will determine what additional information (if needed) is requested on the subsequent pages.

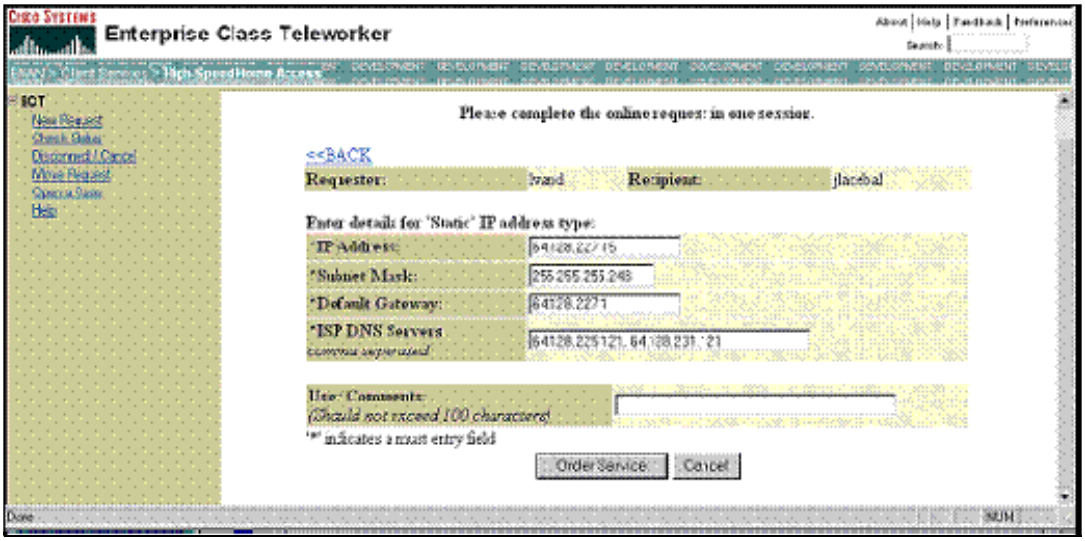
Figure 7. Select Type of E1 Interface



Step 8. If you select "Static", you will be prompted to submit the IP address assignment information needed to configure your Cisco Virtual Office router interface (Figure 8).

Static IP addressing information will be provided by your ISP. Complete all the fields and select "Order Service" to complete your request.

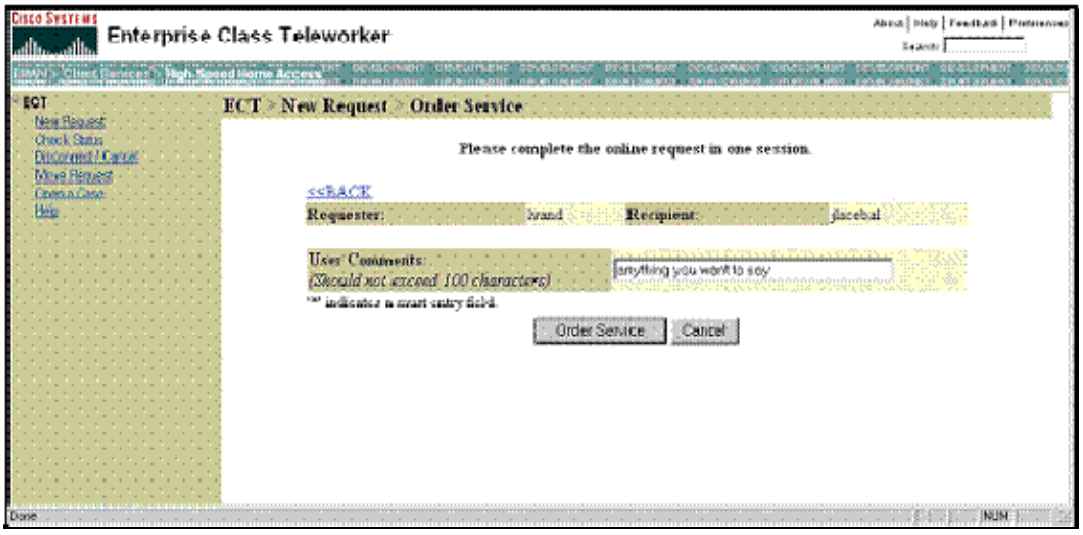
Figure 8. Enter Details for "Static" IP Address Type



Step 9. If you select “DHCP”, you will not be prompted for further information—your Cisco Virtual Office router will obtain an IP address from your ISP via Dynamic Host Control Protocol (DHCP); standard DHCP deployments include all needed routing information.

You have the option to enter comments before ordering the service (Figure 9). Select **“Order Service”** to complete your request process.

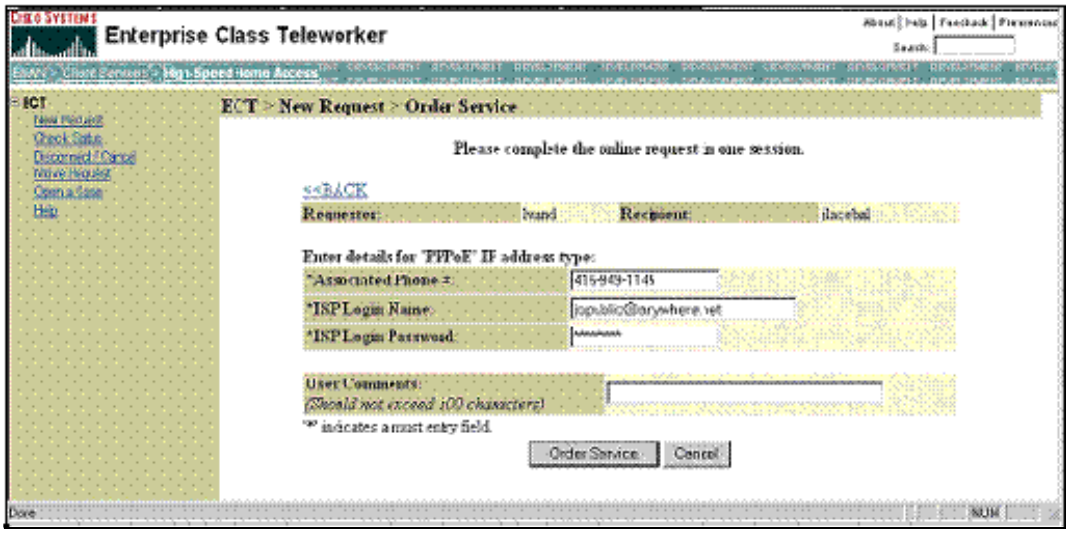
Figure 9. DHCP Select Order Service to Complete Request



Step 10. If you select “PPPoE”, you will be prompted for your ISP login name and password needed to connect to your ISP (Figure 10).

Complete all required information. You have the option to enter comments before ordering the service. Select “Order Service” to complete your request process.

Figure 10. PPPoE Select Order Service to Complete Request



Step 11. Following your submission, your manager will be sent an e-mail to approve your request for the Cisco Virtual Office service. Once approval is received, you will need to order the Cisco Virtual Office router. For complete installation steps, documentation, and more information, please refer to the Learning section.

Manager approval

The completed request form is automatically submitted to the manager who approves the request through an online form. Once the manager has approved the request, the employee is responsible for ordering the VPN router from Cisco, and the router is shipped directly to the employee without involving Cisco IT.

Provisioning begins

Manager approval triggers the Cisco enterprise management system (EMAN) to assign an IP address and a user subnet for the user's home network and to create a login account (user profile) for the new router. This login account will be used by the Cisco Secure Access Control Server (ACS) Solution Engine (formerly known as the AAA server) to authenticate the new router each time it connects. Four types of authentication are used. "Cisco Secure ACS is a generic authentication system," says Kelleher. "But instead of authenticating users, it authenticates devices—the Cisco 800 Series routers." A new Cisco VPN router is also ordered at this time for delivery to the user's home.

Cisco IP Solution Center configuration

EMAN configures IP Solution Center based on Cisco IT security policies and conventions. EMAN passes the subnet address (and the block of 15 addresses) and login account information to IP Solution Center. Based on this information, IP Solution Center generates a configuration for the home VPN router that contains all the security policies, more commonly referred to as service requests, for the router. What used to be a 13-step manual process is now totally automated. For each VPN gateway currently available, Cisco Virtual Office currently uses four types of policies, or sets of Cisco IOS configuration lines These policies include different address translation, QoS, firewall, and IPsec policy variations. Policies, or service requests, are similar for each user, but will vary slightly depending on the user environment, and to uniquely identify each user. For example, the QoS policy will differ from user to user or router to router based on the available bandwidth delivered by the DSL or cable service provider. IP Solution Center includes a feature set [Cert-Proxy] that allows the keys and certificates for the user router to be obtained on behalf of the user router.

Provisioning

The user router is provisioned in two steps: secure "bootstrapping" and security policy push. Bootstrapping provides the router with sufficient configuration to connect the router to a management gateway. It requires ISP access, and the process sets up an IPsec management VPN tunnel, a bootstrap certificate, and a CNS agent configuration to trigger the policy push. In the bootstrap phase, the user connects the new router to the PC and the DSL or cable modem and powers up the PC, which has been assigned an IP address from the DHCP server on the router. The user opens the Web browser and navigates to the router registration form URL. The router responds with the registration page.

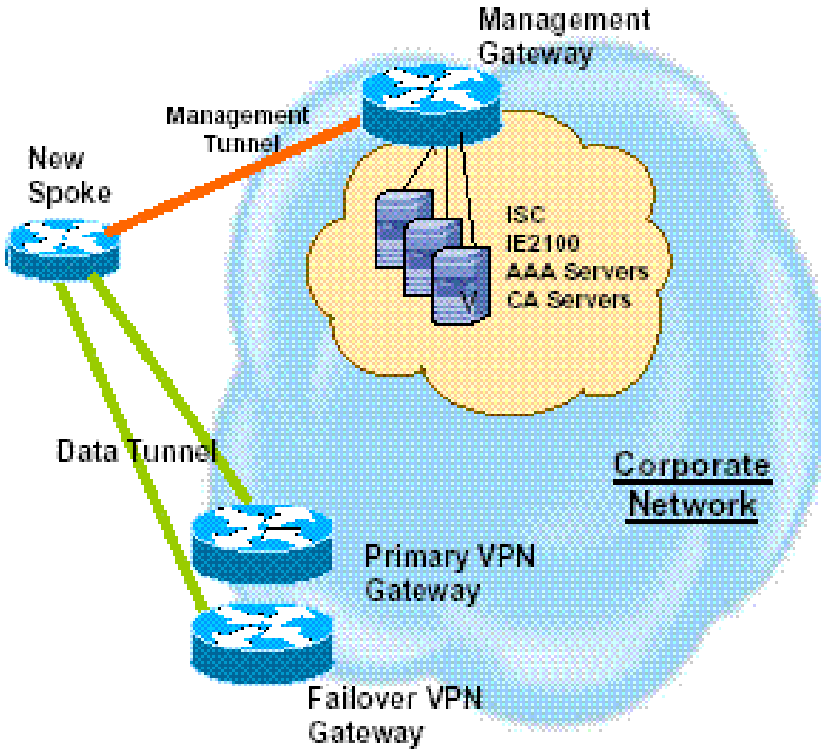
When prompted, the user provides username, password, and Cisco VPN registration URL. This initiates Easy Secure Device Deployment (EZSDD), a simple, Web-based enrollment and configuration-bootstrap interface that allows Cisco IT to deploy a secure network infrastructure in very little time and with no administrator involvement. EZSDD triggers the Cisco Virtual Office deployment using one-time Cisco Secure ACS credentials. The Web browser opens an HTTPS-secured session to the Cisco IT central site server registrar, which verifies the user name with the Cisco Secure ACS server. EZSDD then pushes a bootstrap template and public key infrastructure (PKI) certificate to the new router.

Next, the management tunnel comes up. A CNS agent within the Cisco 800 Series router notifies the Cisco CNS Configuration Engine that the new device has come online, which in turn notifies IP Solution Center. Upon

notification, IP Solution Center pushes all the preconfigured policies it has created to the router. These could include Dynamic Multipoint VPN (DMVPN), Cisco IOS Firewall (Context-Based Access Control [CBAC] and Authentication Proxy [Auth Proxy]), NAT, QoS, Network Admission Control (NAC), and 802.1X. The dual data tunnels are also brought up. At this point, provisioning is complete. The entire process takes about 200 seconds.

Cisco Virtual Office provides for three separate VPN tunnels (Figure 11): a primary and failover tunnel for carrying data, and a management tunnel that is used to monitor the router and manage connections. The data tunnels connect the router to data gateways using Enhanced Interior Gateway Routing Protocol (EIGRP), while the management tunnel connects the router to the Cisco CNS Configuration Engine.

Figure 11. Provisioning a New Cisco Virtual Office Router



IP Solution Center never communicates directly with the router. All communication between the router and IP Solution Center passes through the Cisco CNS Configuration Engine. IP Solution Center understands policies and what needs to be done to provision each router. The Cisco CNS Configuration Engine understands how to turn the policy and configuration into commands to the router to insert the policy into the correct configuration.

Managing Cisco Virtual Office Through Cisco IP Solution Center and CNS Configuration Engine

Cisco IP Solution Center and the Cisco CNS Configuration Engine, together with EMAN, are all part of the ongoing management of Cisco Virtual Office. Within this framework, EMAN is the system of record and single source of “truth”. EMAN includes a unique decision making feature for Cisco Virtual Office called Security Monitor; this feature performs a logic over the environment using what is referred to in mathematics as “regular expressions” and allows automatic decisions based on specific critieria; EMAN performs scheduled configuration changes and ensures the functioning of the Security Monitor feature.

Cisco IP Solution Center is used specifically within Cisco Virtual Office to generate and maintain router configurations and policies, while the Cisco CNS Configuration Engine downloads the configuration and policy information to the

remote router. As in the provisioning process, the configuration engine communicates with the Cisco 800 Series router through a management tunnel, which is separate from the two data tunnels. Following are some of the management tasks that Cisco IP Solution Center and the Cisco CNS Configuration Engine can perform.

Configuration monitoring

Ongoing events that occur on the router are logged by the configuration engine, which is copied to EMAN. Up to two weeks of log data can be accessed by technical support staff through a web interface, providing a rich source of information for resolving operational issues.

IP Solution Center performs triggered audits of what devices are connected and confirms which policies have and have not been successfully pushed out to routers. Any devices whose management tunnels have been disconnected, but whose data tunnels remain active, are noted. Without active management tunnels, routers cannot be monitored.

A single Cisco CNS Configuration Engine can support up to 5000 open connections with user routers. Cisco IP Solution Center supports a feature known as “Fully Managed Service”. Any time a configuration change occurs on a user router, the CNS agent running on the user router notifies the configuration engine. The configuration engine notifies the IP Solution Center, which confirms whether it has authorized the configuration changes in the user router.

These events are reported to EMAN, which notifies the operations team monitoring Cisco Virtual Office. If desired, EMAN automatically disconnects the router if the configuration change violates policies or poses a security threat to the network. In addition, the operations team checks for the existence of the management tunnel. If the management tunnel to a router has failed and policies cannot be checked, the team can terminate the main VPN tunnel.

Configuration changes

When changes are made to any of the standard policies, Cisco IP Solution Center drives these changes, through the configuration engine to the Cisco VPN routers. Password changes are an example. There is no limit on the number of devices that can be modified. And, even if devices are not connected to the network when the configuration changes are pushed out, the configuration engine will push those changes automatically the next time those devices are connected.

Cisco IOS image changes

Finally, the Cisco CNS Configuration Engine can be used to perform image (Cisco IOS Software) upgrades on Cisco VPN routers. “A management system within EMAN allows you to choose 1 to 10,000 routers, select the name of the image you want to push out, hit a button, and the system will send requests off the configuration engine upgrading all the routers,” says Kelleher.

Connectivity

Cisco IP Solution Center and the Cisco CNS Configuration Engine are critical to the provisioning process. Any malfunction of either application will prevent the new user from successfully completing the installation process and connecting to the corporate network. A malfunction will not, however, prevent a router from connecting once the device has been provisioned. The router will continue to send event reports to the configuration engine, but the inability of the configuration engine to receive or act upon those reports does not prevent connection.

Cisco Virtual Office Network Architecture

Cisco IP Solution Center software runs on a UNIX server, while the Cisco CNS Configuration Engine software runs on a Linux-based appliance. There are four Cisco IP Solution Center servers located regionally: two in North America, one in Europe, and one in Asia-Pacific. There are six Cisco CNS Configuration Engine termination points located regionally: four in North America, two in Europe, and one planned for Asiapac.

The reader will note that the headends of data tunnels and management tunnels are not necessarily colocated. For example, the data tunnel for a user in location 1 terminates in location 1, but the management tunnel terminates in

location 2 because that is where the configuration engine server is located. Performance is not affected, however, because data over the management tunnel is only management overhead traffic, which is not noticed by the VPN user.

RESULTS

Through Cisco Virtual Office, Cisco has created a sustainable global deployment and support model capable of meeting the needs of teleworkers around the world. Cisco Virtual Office provides global management capabilities that ensure reliability, availability, and security. Cisco IP Solution Center and the Cisco CNS Configuration Engine have been important components of that solution, providing fast, cost-effective provisioning and ongoing management of Cisco 800 Series integrated services routers. “More than 4200 Cisco employees currently use Cisco Virtual Office, and the number of new users is growing,” says Plamen Nedeltchev, architect of the Cisco IT deployment of Cisco Virtual Office. “With the zero-touch deployment enabled by IP Solution Center and the configuration engine, Cisco can continue to expand Cisco Virtual Office to more and more users.”

LESSONS LEARNED

During the pre-production release of the Cisco Virtual Office solution, Cisco IT added new routers to a common policy. After about 50 routers per policy, however, Cisco IP Solution Center began to experience performance problems. In the production release in August 2004, Cisco IT created a copy of the policy for each new router, so that there was just one router per policy. “We asked the developers if this was feasible, and they said we could have 10,000 individual policies without affecting the system,” says Kelleher.

NEXT STEPS

Cisco IT is currently adding support for templates on the Cisco CNS Configuration Engine, which will be directly managed by EMAN rather than IP Solution Center. Templates are customized configuration commands rather than standard policies; adding this support will allow Cisco Virtual Office management to perform scheduled deployments, rapid deployments, and triggered deployments, essentially covering all types of deployments.

In the future, EMAN will increasingly rely upon the Cisco CNS Configuration Engine to perform more of the configuration management tasks currently handled by legacy tools.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**