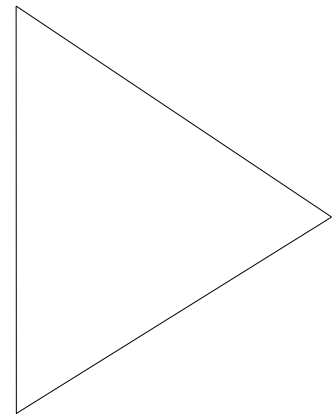


Cisco IOS Lock and Key Security



White Paper

Abstract

The newfound importance and popularity of remote networks pose issues for network managers who administer and impose security policies governing logins from remote sites. Current remote access security solutions were designed for single-user, modem dial-up connections and do not ensure the integrity of data transmissions from remote networks that have multiple users and devices. However, Cisco Systems continues to build on its existing Cisco Internetwork Operating System (Cisco IOS™) security architecture by providing software that allows remote network access only from authenticated remote users.

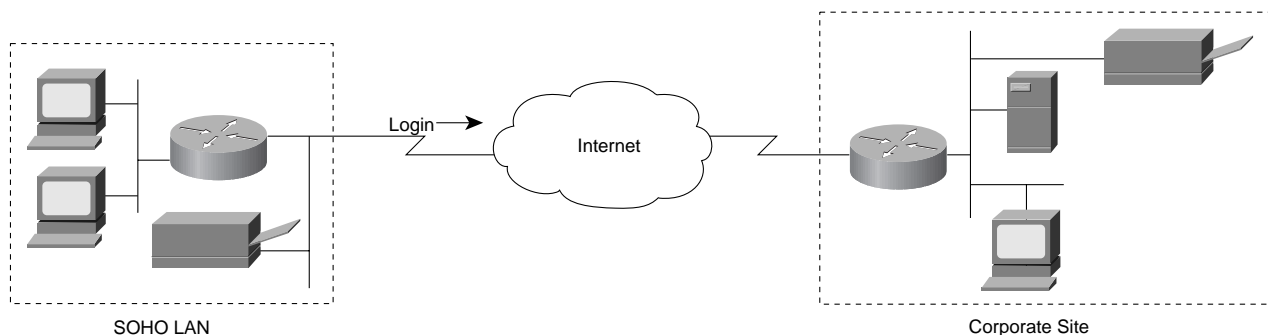
The Shared Resource Challenge

Not long ago, accessing a computer meant sharing time on a mainframe computer. The mainframe architecture provided system managers with extensive control over the computing environment and afforded a centralized security policy. The transformation from the mainframe model of architecture into a distributed client/server architecture was

prompted by several developments. The most important of these developments were the Internet and the Transmission Control Protocol/Internet Protocol (TCP/IP), which made distributed computing possible over local and wide-area networks. The ease of use and popularity of the Internet has increased since the introduction of Web browsers. However, network managers must find ways to protect their computers from unauthorized access over insecure Internet links.

Today's distributed computing has also extended to a mobile world, where workers want access to the corporate site from ever-changing locations. Branch offices with wide-area network (WAN) connectivity also want to provide access and authorization privileges that are unique to each end user. The home office today is changing as well, from a single-user using a dial-up connection such as a modem line or Integrated Services Digital Network (ISDN) service, to a multiple-device telecommuting environment. Many small offices /home offices (SOHO) have local area networks (LANs), and their users want to connect all their resources to a central site. At the corporate site, the network manager must find a way to protect the main corporate computer from unauthorized access (see Figure 1).

Figure 1. Evolving Small Office/Home Office (SOHO) Computing Environments



The shift from the centralized mainframe environment to the distributed client/server environment has forced network managers to move from a central security policy to one that allows for access from remote locations. While remote logging provides flexibility for users, it also poses security problems for the corporate or campus network manager. However, because Lock and Key is implemented on a core router at a central site, it returns centralized control to the network manager.

Current Security Solutions

Today's most common security solution is to use static access control lists—lists manually created by the network manager that define who can access the network—to authenticate and authorize remote users. In today's world, network activity provides the opportunity for break-ins by network hackers. An added vulnerability is that static access lists containing a wide range of network addresses can be stolen by the hacker. Current security solutions exist, but many have drawbacks including the following:

- Firewalls or bastion hosts functioning as gatekeepers at the periphery of a network. This additional equipment is expensive.
- Authentication by means of static access lists. Standard access lists are stored in nonvolatile random-access memory (NVRAM), restrict who can access the system, and provide no challenge mechanism beyond a network address.
- Software solutions that require client software and applications to be modified to support them.

- Application software-based security policies, such as using a specific network application to make connections and send electronic mail and files. There is no methodology to force users to choose a particular application for transmitting sensitive information.

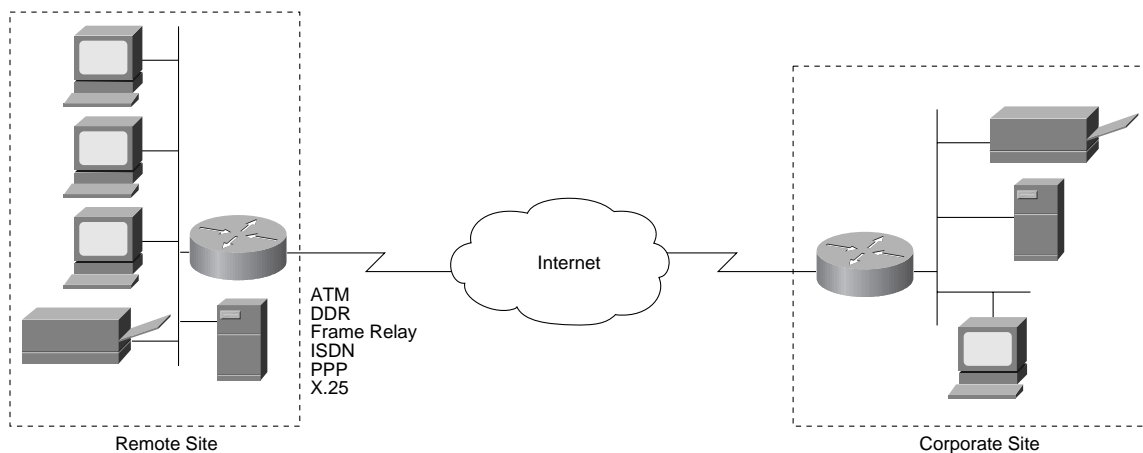
Where multiple systems and applications are in use, security policies based on application layer security are often difficult to enforce. An overlapping security solution approach is prudent; any single security solution is more vulnerable. What is needed is the Lock and Key security software features that Cisco IOS software provides.

Lock and Key—A Dynamic Solution

The Cisco IOS security architecture is based on multiple, overlapping solutions to maintain an organization's security integrity and to provide modular, scalable security. As new technologies become available, the Cisco IOS security architecture is flexible enough to incorporate them.

As part of the Cisco commitment to network security solutions, the Cisco IOS software builds on its security architecture by providing Lock and Key, a solution, that as its name implies, couples access control lists with a challenge/response mechanism that truly challenges users requesting access to a corporate or campus network. Once correct responses are given to the login sequence, which can include a token card identification number, a driver's license number, a maiden name, or other security prompt, Lock and Key allows the remote user access, much as a security guard, viewing a user through a security camera, can open a locked door, permitting access to a building to authorized users and deny it to unauthorized persons.

Figure 2. Lock and Key Supports Any IP-Capable Transmission Mechanism from the Remote Site



Lock and Key Features

Lock and Key offers these features:

- When coupled with TACACS+, allows per-user authorization and authentication in an IP-based, shared media environment at the network layer. Coupling Lock and Key with both TACACS+ and the Challenge Handshake Authentication Protocol (CHAP) on a PPP link provides overlapping security at both the network layer and data link layer.
- Maintains authentication information at a central network access server using technologies such as TACACS, XTACACS, TACACS+, Radius, and Kerberos.
- Provides application independence—Lock and Key does not require modification to user applications.
- Authenticates a user beyond just an IP network address and supports password token cards and other challenge mechanisms for gaining entry to the network.
- Provides a mechanism that requires remote reauthorization during periods of inactivity.

The remote site of today can use many different types of connecting topologies (see Figure 2). Currently, Lock and Key uses the TCP/IP Telnet facility and works well with current WAN technologies. In Figure 2, a user at a remote site can use WAN technology such as Asynchronous Transfer Mode (ATM), dial-on-demand routing (DDR), Frame Relay, ISDN, Point-to-Point Protocol (PPP), or X.25 to connect to the corporate office. The concepts behind the Lock and Key security software make it an ideal solution for securing the campus computer network from the proliferation of Internet users and the corporate network from the proliferation of remote network users.

Because Lock and Key can work with many types of network media, it fits easily into an existing network; you will not need to redesign your network to enable Lock and Key.

How Lock and Key Works

While other authentication solutions were designed for single-user, asynchronous, dial-up services, the trend now is to allow per-user authentication and authorization in shared-media environments, such as a LAN, without requiring special client software. Lock and Key can provide security for a single user, multiple users, and multiple devices in local and remote networks. It does this by using a new type of access list definition.

Access lists are typically created and maintained by manually defining the lists and then distributing them to all other routers in the network. In networks with large

numbers of hosts, this task can be time consuming. These static access lists also consume NVRAM. But most importantly, static access lists do not provide for any challenge mechanisms beyond a network address and password.

Lock and Key uses dynamic access lists that eliminate the need for creating long lists of vulnerable static address information. The network manager creates a template that acts as a placeholder for access definition variables.

The network manager can also control which hosts on a network have access. Timers can be set to automatically delete the access list entry after a certain time, or the network manager can manually clear an entry.

Lock and Key Takes Advantage of the TACACS+ Server

Lock and Key is server independent; however, it is ideally designed for the TACACS+ server. TACACS+ has three components to provide authentication, authorization, and accounting services—protocol support within access servers and routers, protocol specification, and a centralized security database.

Authentication provides the logic for challenging a user login string beyond the standard name and password prompt. Additional query information is defined by the network manager and can be easily and routinely changed to prevent the possibility of a security breach. TACACS+ supports multiple challenge and response strings. For example, TACACS+ can prompt for the user's mother's maiden name or driver license number.

The Lock and Key security mechanism grants system access on a per-user, specific source-destination host basis. This security mechanism is activated only after the user has been authenticated. TACACS+ provides the authentication mechanism. The **autocommand access-enable** command can also trigger a temporary access list stored on the TACACS+ server after the user has successfully authenticated (see Figure 3).

Authorization provides the network manager with control over which parts of a network a user is allowed to use. Per-user access control lists provide the network manager with the ability to support most security policies. Accounting tracks user activity. Reports can be structured to provide user identities.

With TACACS+, all authentication, accounting, and data authorization data is encrypted between the router and the TACACS+ management server. Each TACACS+ service can be tied to its own database or can use other services available on that server or network. The overall design goal

of TACACS+ is to define a standard method for managing dissimilar Network Access Servers (NAS) from a single set of management services such as a database.

Lock and Key Provides Audit Trails and Statistics

Lock and Key supports Access Control List (ACL) reporting solutions, one of which is ACL accounting. Whenever Lock and Key detects that a packet is testing the logic of an access list—perhaps a hacker is trying to violate an access list and exploit the IP addresses it contains—it generates statistical information. This information includes the source and destination of the packet and router response such as blocking or denying the packet. The statistics are kept internal to the router. The Cisco IOS software contains a MIB variable in the accounting portion of the software so that the Simple Network Management Protocol (SNMP) can be used to extract IP access control accounting information and recall violation information.

Lock and Key also supports ACL system logging. Unlike ACL accounting, which keeps internal statistics and reports, statistics and an activity report are transmitted externally to a central site for analysis when a packet tests the logic of an access list by way of the router syslogging facility.

The Cisco IOS Software Supports Multiple Protocol Stacks

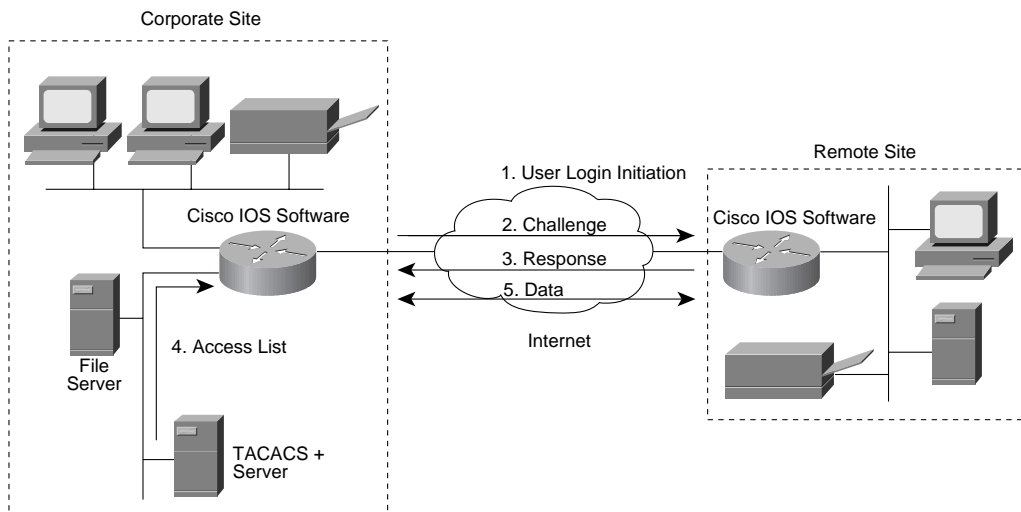
Another current trend for LAN users is to run multiple protocol stacks such as Novell IPX and AppleTalk over Internet Protocol (IP) networks. Although Lock and Key currently supports only IP, with Cisco's Generic Routing Encapsulation (GRE) facility, users can encapsulate most any network protocol into IP. This feature allows users running a network operating system, such as Novell IPX, to be authenticated using their IP addresses and then use that connection to transmit IPX-format data encapsulated in IP format.

Flexible Authentication

Lock and Key has a flexible authentication policy that allows just one, a few, or all systems in a network to be authenticated, thereby allowing a one-time challenge of all systems in a network. The user sets the policy for this feature. Some examples to illustrate this concept follow.

At a branch office of a bank, where only the branch manager is allowed network access, the network manager can define the authentication and authorization policy to accept only that user on the network. In a remote office with a LAN, however, there might be multiple users and devices that need access to the network. The Lock and Key authentication policy can be structured to allow multiple users, as well as multiple devices, to access the network by completing a one-time challenge sequence.

Figure 3. The Lock and Key Login Sequence Goes Beyond Prompting for the Standard Name and Password



Lock and Key Is Easy to Use

Using Lock and Key to log in to a system is easy. In Figure 3, a worker at a remote site uses a router to connect to the corporate network. When logging in from the networked PC attached to the router, Lock and Key challenges the user for some preconfigured test, such as name and password or token card identification number. When the user responds, login information is first checked against that defined by the system manager. Finally, a connection is made that allows data to be securely transmitted between the remote network and the corporate site.

Here is how the session would look at the users' terminal:

```
mysys1% telnet corporate
Trying 127.16.24.1 ...
Connected to corporate.company.com
Escape character is '^]'.
User Access Verification
Name: user
Password:Connection closed by foreign host.
After correct responses are given to the authentication
sequence, Lock and Key creates the temporary access list
entry with access definitions only for the port currently in
use.
```

The temporary entry is removed after a specified idle-timeout or absolute timeout period configured by the system manager, or the system manager can explicitly remove them.

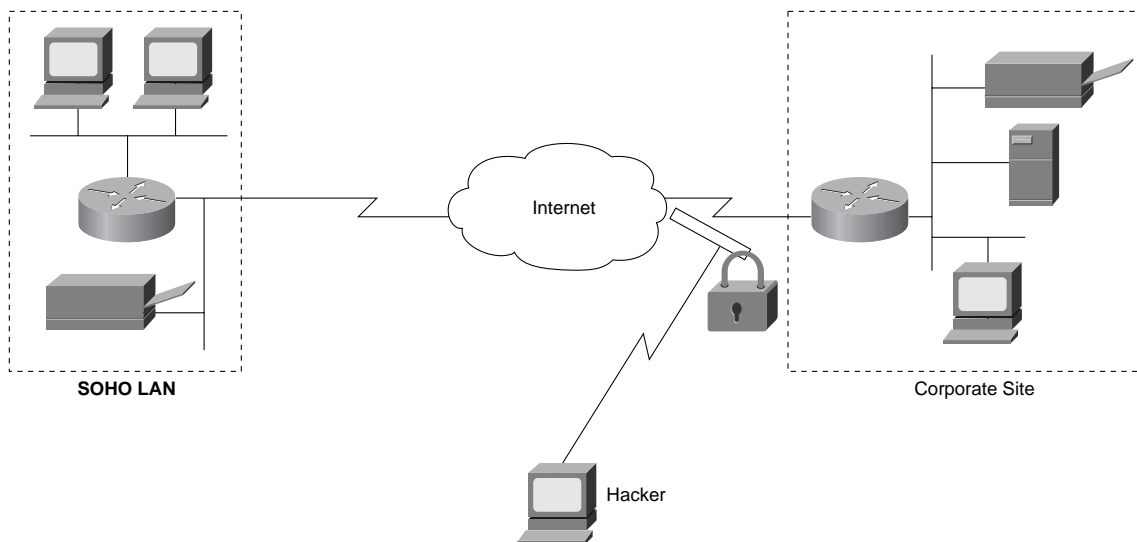
The new Lock and Key access lists can be configured to authenticate a single user or multiple users and devices on a remote LAN, depending on the template defined by the system manager.

Lock and Key Locks Out Network Hackers

Lock and Key locks out network hackers and effectively plugs possible holes that would allow intruders into the corporate network by locking out all incoming traffic until the user login information has been authenticated at the corporate site, and only permitting access for a specific port.

Spoofing is the primary method that hackers use to break into network systems. Figure 4 shows how a potential hacker trying to gain access would have to dial in to the same port after the connection went down and spoof the same host and network address. The temporary access lists and time limits set for user access significantly reduce hackers' opportunities for doing this. The hacker's window of opportunity can be even further reduced by incorporating CHAP at the data link. This imposes that a hacker would have to break through CHAP in addition to performing IP address spoofing.

Figure 4. Hackers Are Thwarted When Trying to Break into a Network That Uses the Lock and Key Access Control.



A new **access-list** command option specifies the Lock and Key access list entry. This prevents the network manager from having to create hundreds of access list definitions that may not be used, and it reduces NVRAM memory requirements. A new command, **autocommand access-enable**, triggers the temporary access list only after the user has correctly answered the authentication challenge.

The Cisco IOS Security Solutions Lead the Way

Cisco Systems leads the way in providing security solutions for today's remote LANs. The Cisco IOS with Lock and Key security software feature provides key capabilities for securing remote networks—dynamic access lists and a robust server that provides query logic and monitoring functions. Best of all, Lock and Key fits easily into existing networks without additional equipment or cumbersome topology reconfiguration.

0496R



Cisco Systems Worldwide Offices

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

World Wide Web URL:
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco Systems has more than 125 sales offices worldwide. To contact your local account representative, call Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic - Batiment L2
16, Avenue du Quebec
BP 706 Villebon
91961 Courtaboeuf Cedex
France
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Intercontinental and Latin American Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-7660
Fax: 408 526-4646

Japanese Headquarters

Nihon Cisco Systems K.K.
Seito Kaikan 4F
5, Sanbancho, Chiyoda-ku
Tokyo 102
Japan
Tel: 81 3 5211 2800
Fax: 81 3 5211 2810

Austria

Cisco Systems Austria GmbH
World Trade Center
A-1300 Vienna Airport
Austria
Tel: 43 1 7007 6256
Fax: 43 1 7007 6027

Belgium
Cisco Systems Bruxelles
Complex Antares
71 avenue des Pleiades
1200 Brussels
Belgium
Tel: 32 2 778 42 00
Fax: 32 2 778 43 00

Denmark

Cisco Systems
Larsbjornsstraede 3
Dk-1454 Copenhagen K
Denmark
Tel: 45 33 37 71 57
Fax: 45 33 37 71 53

Finland

Cisco Systems
Maistraatiportti 2A
FIN-00240 Helsinki
Finland
Tel: 358 1594 3090
Fax: 358 1594 3093

Germany

Cisco Systems GmbH
Max-Planck-Strasse 7, 3rd Floor
85716 Unterschleißheim
Germany
Tel: 49 89 32 15070
Fax: 49 89 32 150710

Ireland

Cisco Systems Ltd.
Europa House, 4th Floor
Harcourt Street
Dublin 2
Ireland
Tel: 35 3 1 475 4244
Fax: 35 3 1 475 4778

Italy

Cisco Systems Italy Srl
Centro Direzionale Milano Oltre
Palazzo Raffaello Scala B 4P
Via Cassanese 224
20090 Segrate (Mi)
Italy
Tel: 39 2 26 97 31
Fax: 39 2 26 92 9006

The Netherlands

Cisco Systems
Stephensonweg 8
4207 HB Gorinchem
The Netherlands
Tel: 31 183 622 988
Fax: 31 183 622 404

Norway

Cisco Systems
Holmens Gate 4
N-0250 Oslo
Norway
Tel: 47 22 83 06 31
Fax: 47 22 83 22 12

Portugal

Cisco Systems Portugal
Avda. da Liberdade 114-134
1250 Lisboa
Portugal
Tel: 351 1 340 45 31/2
Fax: 351 1 340 4575

South Africa

Cisco Systems South Africa
Meintjie Parker House
328 Rivonia Blvd.
Rivonia, Gauteng
South Africa
Tel: 27 11 807 4444
Fax: 27 11 807 4447

Spain

Cisco Systems Spain
Avenida de Burgos, 17 Pl. 11
Edificio Triada II
28036 Madrid
Spain
Tel: 34 1 383 2178
Fax: 34 1 383 8008

Sweden

Cisco Systems AB
Arstaangsvagen 13
117 60 Stockholm
Sweden
Tel: 46 8 681 41 60
Fax: 46 8 19 04 24

Switzerland

Cisco Systems Switzerland
Grossrietstrasse 7
CH-8606 Naenikon/ZH
Switzerland
Tel: 41 1 905 20 50
Fax: 41 1 941 50 60

United Arab Emirates

Cisco Systems (Middle East)
PO Box 26095
City Tower 2
Sheik Zayed Road
Dubai, UAE
Tel: 971 4 318 788
Fax: 971 4 313 681

United Kingdom

Cisco Systems Ltd.
4 New Square
Bedfont Lakes
Feltham, Middlesex TW14 8HA
UK
Tel: 44 1 81 818 1400
Fax: 44 1 81 893 2824

Norway

Cisco Systems
Holmens Gate 4
N-0250 Oslo
Norway
Tel: 47 22 83 06 31
Fax: 47 22 83 22 12

Asia

Cisco Systems (HK) Ltd
Suite 1009, Great Eagle Centre
23 Harbour Road
Wanchai
Hong Kong
Tel: 852 2583 9110
Fax: 852 2824 9528

Cisco Systems (HK) Ltd
Beijing Office
Room 821/822, Jing Guang
Centre
Hu Jia Lou, Chao Yang Qu
Beijing 100020
China, PRC
Tel: 86 10 501 8888 x821/822
Fax: 86 10 501 4531

Cisco Systems (HK) Ltd
New Delhi Liaison Office
Suite 119, Hyatt Regency Delhi
Bhikai Cama Place, Ring Road
New Delhi 110 066
India
Tel: 91 11 688 1234 x119
Fax: 91 11 611 7688

Cisco Systems, (HK) Ltd
Level 12, Wisma Bank
Dharmala, JI
Jenderal Sudirman Kav. 28
Jakarta Selatan 12910
Indonesia
Tel: 62 21 523 9132
Fax: 62 21 523 9259

Cisco Systems Korea
Samik Ravidol Building 5th
floor
720-2 Yuksam-2-dong,
Gangnam-ku
Seoul, 135-082
Korea
Tel: 82 2 3453 0850
Fax: 82 2 3453 0851

Cisco Systems (HK) Ltd
Kuala Lumpur Office
Level 5, Wisma Goldhill
67 Jalan Raja Chulan
50200 Kuala Lumpur
Malaysia
Tel: 60 3 236 5147
Fax: 60 3 236 5146

Cisco Systems Manila Office
The Executive Tower Centre
Room 9, 24/F, Pacific Star
Building
cor. Buendia Street, Makati
Avenue
Makati City
Philippines
Tel: 632 892 4476
Fax: 632 811 5998

Cisco Systems (USA) Pte Ltd
501 Orchard Road
#04-11 Lane Crawford Place
Singapore 238880
Tel: 65 738 5535
Fax: 65 738 2202

Cisco Systems (HK) Ltd
Taipei Office
4F, 25 Tunhua South Road,
Section 1
Taipei
Taiwan, ROC
Tel: 88 62 577 4352
Fax: 88 62 577 0248

Cisco Systems (HK) Ltd
7th Floor, The Park Place
Building
231 Sarasin Road, Pathumwan
Bangkok 10330
Thailand
Tel: 662 253 5315
Fax: 662 253 8440

Argentina

Cisco Systems Argentina
Cerrito 1054, Piso 9
(1001) Buenos Aires
Argentina
Tel: 54 1 811 7526
Fax: 54 1 811 7495

Australia

Cisco Systems Australia Pty Ltd
Level 17
99 Walker Street
North Sydney NSW 2060
Australia
Tel: 61 2 9935 4100
Fax: 61 2 9957 4077

Brazil

Cisco Systems Do Brasil
Rua Helena 218, 10th Floor
Cj 1004-1005 Vila Olimpia
Sao Paulo, SP CEP 04552-050
Brazil
Tel/Fax: 55 11 822 6095
Tel/Fax: 55 11 822 6396

Canada

Cisco Systems Canada Limited
150 King Street West
Suite 1707
Toronto, Ontario M5H 1J9
Canada
Tel: 416 217-8000
Fax: 416 217-8099

Central America / Caribbean

Cisco Systems, Inc.
790 NW 107th Avenue, Suite
102
Miami, Florida 33172
USA
Tel: 305 228-1200
Fax: 305 222-8456

Colombia

Cisco Systems Colombia
Cra. 18 #86A-14
Bogota
Colombia
Tel: 57 1 296 0067
Fax: 57 1 616 3030

Mexico

Cisco Systems de México, S.A.
de C.V.
Ave. Ejecito Nacional No. 926
Ser Piso
Col. Polanco C.P. 11560
Mexico D.F.
Tel: 52 5 328 7600
Fax: 52 5 328 7699

New Zealand

Cisco Systems New Zealand
Level 16, ASB Bank Centre
135 Albert Street
P.O. Box 6624
Auckland
New Zealand
Tel: 64 9 358 3776
Fax: 64 9 358 4442

Venezuela

Cisco Systems Venezuela
Calle Bajada de Los Curtidores
Qta. Jakaranda - Alto Hatillo
Caracas
Venezuela
Tel/Fax: 58 2 963 6140
0396R

Cisco Systems and Cisco IOS are trademarks, and Cisco and the Cisco logo are registered trademarks of Cisco Systems, Inc. All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. 0196R