Deployment Guide

Deployment of Cisco IP Mobility Solution on Enterprise Class Teleworker Network

The Cisco® Service Oriented Network Architecture (SONA) framework helps enterprise customers evolve their existing infrastructure into an Intelligent Information Network that supports new IT strategies, including service-oriented architecture, Web services, and virtualization. By integrating advanced capabilities enabled by intelligent networks, enterprises can reduce complexity and management costs, enhance system resiliency and flexibility, and improve usage and efficiency of networked assets.

Part of the SONA framework, the Cisco Enterprise Class Teleworker (ECT) solution securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations.

Emerging wireless technologies such as wireless LANs and 3G make it possible for enterprise teleworkers to access their intranet from virtually anywhere, and at any time. For example, a teleworker can move from an Ethernet-connected docking station in a home office to a Wi-Fi-enabled living room; from a Wi-Fi-enabled train station to a 3G-enabled moving metro train; or from a Wi-Fi-enabled office to a Wi-Fi-enabled meeting room.

While ubiquitous IP connectivity is becoming more of a reality, some challenges remain. Today, a mobile device can have Wi-Fi, 3G, and Ethernet connections, but it is still unclear which is best to use in a given instant, when all are available. And while multiple wireless technologies can be used to cover a mobile user's work areas, switching between these technologies can result in frozen or restarted applications, disconnected VPNs, and dropped packets. This can affect enterprise productivity and diminish the benefits of pervasive wireless and IP connectivity.

This deployment guide addresses how Cisco IOS IP Mobility technology can be integrated into the ECT solution framework to enable teleworkers to roam between networks while enjoying secure connectivity to the corporate intranet without service interruption. This guide explores the various options available to commercial and enterprise customers looking to integrate mobility and security into their networks.

BACKGROUND

Cisco IOS IP Mobility technology provides mobile users with a simple, user-intervention-free experience to gain network connection anywhere, at any time. It provides intelligent connection management for users by automatically selecting the "best" access link whenever possible without user intervention. Session continuance helps increase user productivity and reduces the frustration of having to restart applications.

Cisco IOS IP Mobility technology uses the IETF Mobile IP standard to enable users to freely move from one location to another and to switch between networks without worrying about application sessions being dropped. Mobile IP technology also simplifies solution interoperability. Cisco IOS IP Mobility technology includes the Cisco Mobile Wireless Home Agent, Cisco IOS Foreign Agent, Cisco Mobile Router, and Cisco Mobile Client. This documentation focuses on using the Cisco Mobile Wireless Home Agent and the Cisco Mobile Client. For more information about Cisco IOS IP Mobility technology, visit: http://www.cisco.com/en/US/products/ps6551/products_ios_technology_home.html

The Cisco ECT solution provides a Cisco IOS® Software-based large-scale, secure, end-to-end managed IP network with integrated managed services and applications support. It provides a standard solution for facilitating secure network integration to suppliers, partners, employees, and customers. The Cisco ECT solution supports global deployment and a management model that provides a low total cost of ownership (TCO). More details on the Cisco ECT solution can be found at: http://cisco.com/go/ect

Cisco Easy VPN and Cisco IOS SSLVPN are e two ECT components that can be used in the IP mobility solution. Cisco Easy VPN is a Cisco IOS Software-based VPN solution that simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client Framework, the Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, thus reducing the management complexity of VPN deployments.

Cisco IOS SSLVPN provides remote secure corporate network (intranet) access over the standard public Internet using only a Web browser and its native Secure Sockets Layer (SSL) encryption. An SSL-enabled Web browser can be used to access e-mail, the intranet, and various applications and resources inside the corporate network from any PC.

Integrating Mobile IP technology with the Cisco ECT solution framework provides seamless roaming between different networks while keeping a secure VPN connection to the corporate network.

TARGET MARKET SEGMENTS

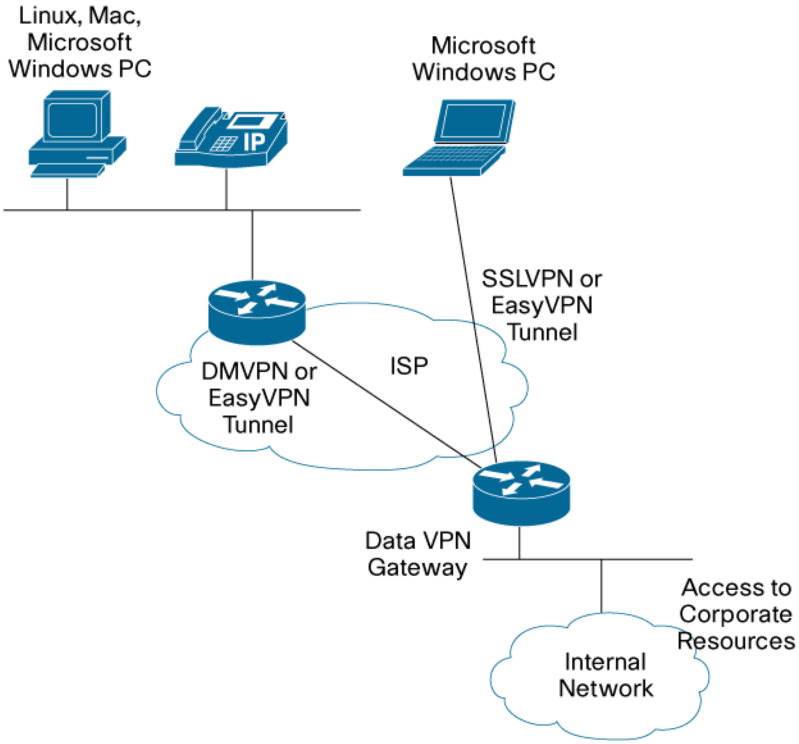
This secure Mobile IP solution is ideal for both enterprise and commercial business segments. In enterprise networks, this solution provides secure access to employees even from roaming locations; for example, commuting employees or sales personnel can maintain connectivity to their corporate network without having to re-establish sessions while moving from place to place.

Commercial companies find this solution useful when, for example, remote users in professions such as retail brokerage for financial institutions need to securely access the corporate servers of the parent company while visiting their clients. As another example, a banking professional could access the headquarters to get an instant loan approval or identify current interest rates.

NETWORK ARCHITECTURE

Figure 1 shows the components of the Cisco ECT solution base architecture that is used in this IP mobility solution. Cisco Easy VPN or Cisco IOS SSLVPN give end users secure access to corporate resources.

Figure 1. Original Cisco ECT Topology



Platform and Images

Following are the components and versions used in an IP mobility deployment of the Cisco ECT solution.

- Cisco Mobile Wireless Home Agent: Cisco 7200 or 7300 Series Router using the –js- image with Cisco IOS Software Release 12.4(6)T1
- VPN gateway: Cisco 7200 Series Router or Cisco 3845 Integrated Services Router using the adventerprisek9 image with Cisco IOS Software Release 12.4(6)T1
- Cisco Mobile Client Version 2.0.14
- Cisco Easy VPN Client Version 4.0.5
- Cisco IOS SSLVPN Client Version 1.0.2.127
- Cisco Secure Access Control Server (ACS) Version 4.0

Cisco IOS IP Mobility Components

Cisco Mobile Client

The Cisco Mobile Client provides intelligent roaming between wired and wireless networks, enabling all application sessions to continue without user intervention or application restarts. For more information about Cisco Mobile Client, visit: http://www.cisco.com/en/US/products/ps6527/tsd_products_support_series_home.html

To download the Cisco Mobile Client, visit http://www.cisco.com/cgi-bin/tablebuild.pl/cmc-1.0. This site will require a Cisco.com ID.

Cisco Mobile Wireless Home Agent

To offer seamless roaming to customers, mobile operators need an IP connection that is always on, independent of location, movement, or wireless infrastructure. They also need quality of service (QoS) capabilities, especially the ability to forward packets at rates appropriate for each connection. For example, if a user connects to a wireless WAN and then roams to a faster 3G network, the mobile operator needs to reduce the packet-forwarding rate at the moment the new connection takes over, in order to avoid packet loss (from too high a forwarding rate) or sub-optimal performance (from too low a forwarding rate). The Cisco Mobile Wireless Home Agent is based on the IETF Mobile IP standard (RFC 3344), which identifies a host device by a single IP address even if the device moves its physical point of attachment from one network to another. The result: subscribers with mobile devices can roam to another network without restarting applications or terminating and re-establishing a connection.

Cisco ECT Solution Components

Cisco Easy VPN and Cisco IOS SSLVPN are the ECT solution components that can be used for implementing a secure Mobile IP network deployment.

The VPN gateway in the corporate network can be a Cisco Easy VPN gateway or a Cisco IOS SSLVPN gateway. When registering with the Cisco Easy VPN gateway, the user can use pre-shared keys or certificates. The Cisco Easy VPN hub can also be configured for split tunneling, which allows only corporate traffic to pass through the VPN gateway. All other traffic can be directed to the Internet directly from the Cisco Mobile Wireless Home Agent. When the VPN gateway is a Cisco IOS SSLVPN gateway, it can operate in full tunnel mode, clientless mode, or thin client mode.

When a VPN gateway is mentioned in this document, it is either a Cisco Easy VPN gateway, a Cisco IOS SSLVPN gateway, or a converged VPN gateway that supports both VPN technologies.

Cisco Easy VPN Client (VPN Client)

A VPN session can be established over the Mobile IP connection originating from the user’s laptop. The VPN gateway is beyond the home agent; all packets to the corporate network are encrypted from the laptop and are routed through the home agent. As the user roams, the Mobile IP tunnel is maintained (as long as there is network connectivity in the area). The VPN session is maintained and all the applications run without interruption. For more information on Cisco Easy VPN deployment, visit: http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd80267995.shtml

Cisco IOS SSLVPN Client (SSL VPN Client)

Cisco IOS SSLVPN provides remote secure corporate network (intranet) access over the standard public Internet using only a Web browser and its native Secure Socket Layer (SSL) encryption. SSL authentication and encryption/decryption operates at the application level, which eliminates the need for any special-purpose software installation at the client side. An SSL-enabled Web browser and e-mail client can be used to access e-mail, the corporate intranet, and various applications and resources inside the corporate network. The end host supporting the browser could be any IP-based host (PC, Mac, Linux/UNIX).

When users are mobile and have a Mobile IP session established, they can start the Cisco IOS SSLVPN session using a browser in clientless or full tunnel mode. Once the session is successfully established, they can access the corporate resources. For more information on Cisco IOS SSLVPN deployment, visit: http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd8029d630.shtml

CISCO ECT AND MOBILE IP SOLUTION

Security Challenges When Using Cisco Mobile Client Alone

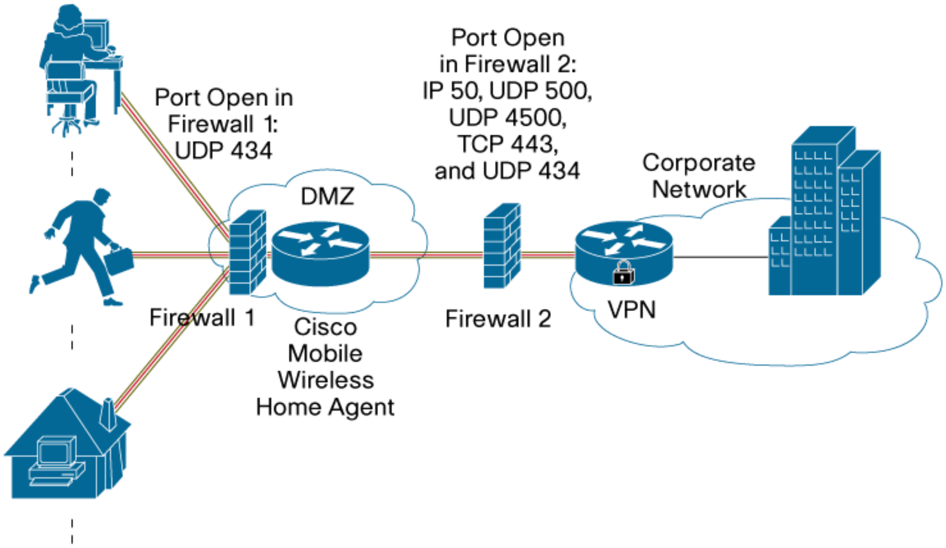
When Cisco Mobile Client is used from the laptop, it registers with the home agent in the corporate network. This requires that the User Datagram Protocol (UDP) port 434 be open in the firewall between the Internet and corporate network for handling the Mobile IP traffic. There is no control on the type of traffic that passes through the Mobile IP tunnel. Users can send malicious data inside the Mobile IP packet and disrupt the corporate network.

Adding Security to the Solution

Integrating Mobile IP with Cisco Easy VPN or Cisco IOS SSLVPN provides a way to secure the traffic flowing into the corporate network. The Cisco Mobile Wireless Home Agent can be placed in the DMZ. This allows for UDP port 434 alone to be opened in the firewall between the Internet and DMZ, and does not compromise the entire corporate network. The VPN gateway can be placed in the corporate network and the corresponding ports (SSLVPN: TCP 443 and IP Security [IPsec]: IP 50, UDP 500, and UDP 4500) can be opened in the firewall between the DMZ and the corporate. This allows only encrypted traffic to flow into the corporate network. Figure 2 shows a conceptual view of Mobile IP tunnel and VPN tunnel being up when the user is roaming.

The Cisco Mobile Client on the laptop registers with the home agent. Upon successful registration, a VPN session can be established with the VPN gateway. Any traffic to the corporate network will now be encrypted. All other data traffic destined toward the Internet will go to the home agent and then go directly to the Internet if split tunneling is enabled on the VPN gateway.

Figure 2. Conceptual View of Mobile IP Tunnel and VPN Tunnel Being Up When User Is Roaming

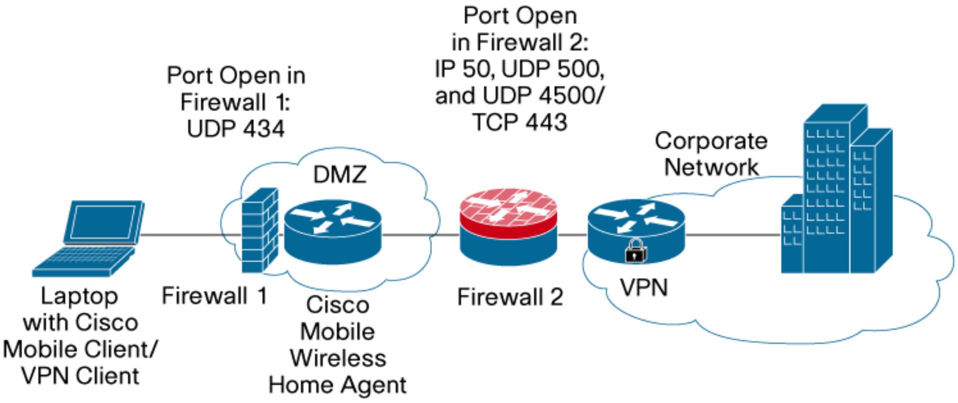

Port Open in Firewall 1: UDP 434
Port Open in Firewall 2: IP 50, UDP 500, UDP 4500, TCP 443, and UDP 434
DMZ
Corporate Network
Firewall 1
Cisco Mobile Wireless Home Agent
Firewall 2
VPN

DEPLOYMENT SCENARIOS

This section explains the possible deployment scenarios using the Cisco Mobile Wireless Home Agent and a VPN gateway.

Cisco Mobile Wireless Home Agent in DMZ and VPN Gateway in Corporate Network (External Roaming Only)

Figure 3. Network Topology with Cisco Mobile Wireless Home Agent in DMZ and VPN Gateway in Corporate Network


Port Open in Firewall 1: UDP 434
Port Open in Firewall 2: IP 50, UDP 500, and UDP 4500/ TCP 443
Corporate Network
DMZ
Laptop with Cisco Mobile Client/ VPN Client
Firewall 1
Cisco Mobile Wireless Home Agent
Firewall 2
VPN

As shown in Figure 3, the Cisco Mobile Wireless Home Agent resides in the DMZ and the VPN gateway resides in the corporate network. The advantage of this design is that only UDP port 434 needs to be opened in the firewall between the Internet and DMZ. This prevents any major damage to the corporate network. The traffic destined for the corporate network then passes through another firewall (which has only ports for VPN gateway open) to terminate VPN sessions on the VPN gateway. This way only legitimate user traffic comes to the corporate network.

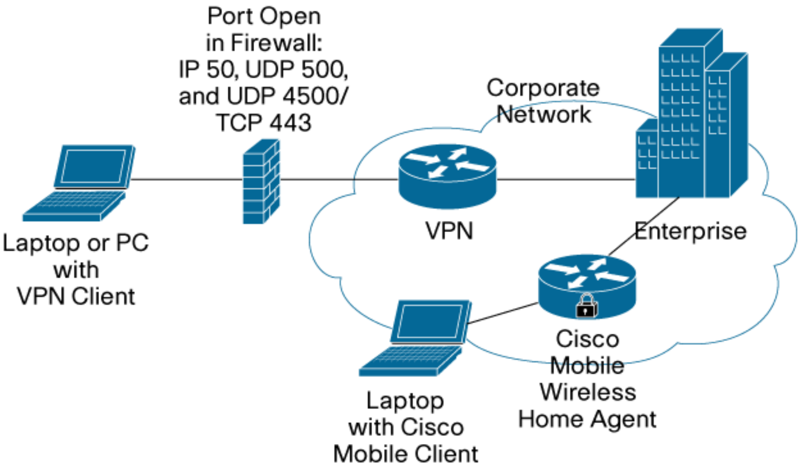
This is one of the most secure designs available. The disadvantage of this design is that it supports only external roaming, i.e., only users that are outside the corporate network and are roaming can maintain session continuance. When entering the corporate network, the user has to manually disconnect the Cisco Mobile Client to be able to access the corporate network.

The security of the Cisco Mobile Wireless Home Agent itself can be increased by using a combination of access control lists and the Cisco IOS Software Flexible Packet Matching feature. The Flexible Packet Matching feature in Cisco IOS Software can be used to deny any traffic that is not encrypted. Flexible Packet Matching allows the packet contents to be examined at a particular offset for a particular pattern. Policies can be configured on the router, which allows the router to drop the packet if the Mobile IP header is not followed by an IPsec header.

Cisco Mobile Wireless Home Agent and VPN Gateway in Corporate Network (Internal Roaming Only)

The Cisco Mobile Wireless Home Agent and the VPN gateway can reside in the corporate network and only allow internal roaming. Internal roaming is useful for moving between different internal networks; for example, between different corporate buildings. Figure 4 shows an example of internal roaming.

Figure 4. Network Topology with Cisco Mobile Wireless Home Agent and VPN Gateway in Corporate Network


Port Open in Firewall: IP 50, UDP 500, and UDP 4500/ TCP 443
Corporate Network
Laptop or PC with VPN Client
VPN
Enterprise
Cisco Mobile Wireless Home Agent
Laptop with Cisco Mobile Client

When inside the corporate network, the user registers with the internal home agent address. Once the Mobile IP session is established, the user can move between internal networks without losing application sessions.

In this scenario, the traffic does not need to pass through the corporate firewall, so no firewall ports need to be opened. The VPN gateway is used for external VPN access, but external roaming is not possible, as the home agent is only reachable from the internal network.

CONFIGURATION

Firewall Configuration

Firewall configuration for permitting Mobile IP traffic:

```
permit udp any host 10.1.1.1 eq 434
```

Firewall configuration for permitting IPsec traffic:

```
permit ip any host 10.3.1.1 eq 50
permit udp any host 10.3.1.1 eq 500
permit udp any host 10.3.1.1 eq 4500
```

Firewall configuration for permitting Cisco IOS SSLVPN traffic:

```
permit tcp any host 10.3.1.1 eq 443
```

Cisco Mobile Wireless Home Agent Configuration

```
router mobile
!
ip local pool NAI-POOL 10.1.2.1 10.1.2.255
ip mobile home-agent address 10.1.1.1 broadcast lifetime 1800 nat-detect replay 255
ip mobile host nai @mycompany.com address pool local NAI-POOL interface GigabitEthernet0/0
ip mobile secure host nai @mycompany.com spi 234 key hex 0089786512345987611116153412131
algorithm md5 mode prefix-suffix
!
```

Cisco Mobile Client

The Cisco Mobile Client build can be found at http://www.cisco.com/cgi-bin/tablebuild.pl/cmc-1.0. This site requires a Cisco.com ID.

Details on setting up Cisco Mobile Client to interact with the Cisco Mobile Wireless Home Agent can be found in the user guide at: http://www.cisco.com/en/US/products/ps6527/tsd_products_support_series_home.html

APPENDIX

Full configuration of the Cisco Mobile Wireless Home Agent:

```
ha#sh run
Building configuration...

Current configuration : 2550 bytes
!
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ha
!
boot-start-marker
boot system disk0:c7301-adventerprisek9-mz.124-6.T
boot-end-marker
!
enable secret 5 1234567
!
aaa new-model
!
!
!
aaa session-id common
!
resource policy
```

```
!
clock timezone PST -8
clock summer-time PDT recurring
ip cef
!
!
!
!
no ip domain lookup
ip domain name cisco.com
ip multicast-routing
!
!
password encryption aes
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router mobile

ip local pool NAI-POOL 10.1.2.1 10.1.2.255
ip mobile home-agent address 10.1.1.1 broadcast lifetime 1800 nat-detect replay 255
ip mobile host nai @mycompany.com address pool local NAI-POOL interface GigabitEthernet0/0
ip mobile secure host nai @mycompany.com spi 234 key hex 0089786512345987611116153412131
algorithm md5 mode prefix-suffix

logging alarm informational
```

```
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 120 0
 transport input ssh
 transport output ssh
 stopbits 1
!
ntp clock-period 17179980
ntp update-calendar
!
end

ha#
```

REFERENCES

For more information on the Cisco ECT solution, visit: http://www.cisco.com/go/ect/

For more information on Cisco Easy VPN configuration, visit:
http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd80267995.shtml

For more information on Cisco IOS SSLVPN gateway configuration, visit:
http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd8029d630.shtml

For more information on Cisco Mobile Client, visit:
http://www.cisco.com/en/US/products/ps6527/tsd_products_support_series_home.html

For more information on IOS SSLVPN feature and products, visit: http://www.cisco.com/go/iossslvpn

CISCO SYSTEMS

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.
168 Robinson Road
#28-01 Capital Tower
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.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

Printed in USA C07-362637-00 08/06