Datasheet

Cisco Mobile Client for Windows 2000, XP

Last Updated: April 2006

CISCO MOBILE CLIENT OVERVIEW

The Cisco Mobile Client (CMC) is an easy to use middleware application that allows a user the ability to keep a laptop or tablet device connected while roaming between wired and wireless connections. CMC is targeted at Enterprise customers that have workers that transition from various wired and wireless connections during the course of a day. It can also be used by users who want to seamless roam across Internet when they move between access networks such DSL, home WiFi networks, and cellular wireless data networks.

CMC offers Enterprise customers:

- An intelligent connection manager in an easy to use Windows based client for a single device such as a laptop or Tablet PC
- A standard based Mobile IPv4 client for seamless roaming without user intervention , between wired and wireless links
- Compatibility with the Cisco VPN client and its VPN infrastructure, enabling a Mobile VPN solution that provides secure mobile connectivity

CMC is part of the Cisco suite of standards based Mobile IP (MoIP) solutions, which consists of Cisco Home Agent Routers, Cisco Packet Data Serving Nodes (PDSN), Cisco Foreign Agent Routers, the Cisco 3200 Series Wireless and Mobile Router, and the Cisco Mobile Client. The Cisco Mobile Client is also a key component of the Cisco Mobile VPN solution, where an extra security layer is provided on top of the Mobile IP layer by using Cisco VPN solutions—the Cisco VPN client and Cisco VPN concentrators/routers.

In a Mobile IP network, CMC is an ideal companion for Cisco 3200 Series Wireless and Mobile Router. The Cisco 3200 Series routers connects multiple devices on a vehicle for mission critical public safety, transportation and defense networks or it can be used as an outdoor wireless router. CMC can be enabled on the devices that typically roam together with the Cisco 3200 Routers, when they need to roam between Cisco 3200 Series Wireless and Mobile Routers and in between vehicles or when located outdoors.

FEATURE SUPPORT

The areas of features supported by the Cisco Mobile Client include:

- Intelligent connection management in familiar Windows based software
  - Network connection management functionality
  - Client configuration and profile management
  - Software OS support
- Seamless roaming based on standard Mobile IP (RFC 3344)
  - Basic and advanced Mobile IP features
  - Interoperability with the Cisco Mobile IP infrastructure
- Secure Mobility
  - CiscoVPN client interaction
  - Compatible with the Cisco security infrastructure
  - Additional features added for client software security

INTELLIGENT CONNECTION MANAGEMENT IN WINDOWS BASED SOFTWARE

Network Connection Management Functionality

Interface Priority List

The CMC detects all existing interfaces on the mobile device at the time of installation and detects all interfaces that are installed at a later time. As interfaces become active they are available for use in mobility provision. All installed interfaces can be prioritized based on preference. By default, interfaces are ordered based on their advertised speeds. For example, a 100-MB Ethernet interface would have a higher priority than an 802.11a/b/g WLAN interface. However, this ordering can be changed using the Graphical User Interface (GUI). Dial-up connectivity can also be included in this list and prioritized as needed.

Handover on WLAN-Signal Strength

Configurable either through the CMC profile or through the GUI, it is possible to specify thresholds for WLAN access whereby a PPP connection will be established automatically if the signal strength on the adapter decreases. As WLAN signal strength decreases below a first threshold, a PPP connection is established. If the signal strength continues to decrease below a second level, a handover will occur to the established PPP connection. In reverse, if the WLAN signal strength increases above the lower threshold, handover will occur back to the WLAN interface. If signal strength continues to increase above the second threshold, the PPP connection is torn down. The monitoring of the WLAN signal strength is cumulative, taking into account the trend over a period of time (over several seconds), avoiding any handovers due to spikes on the WLAN network.

Auto-Dial

Auto-dial is also available, the CMC will establish a PPP connection (of choice) if connectivity over interfaces of higher priority is not possible. In this case, the CMC can be configured to dial the connection automatically, or prompt the user for confirmation before establishing the connection. If a higher priority connection becomes available, the CMC will switch to this connection and drop the PPP connection.

Re-Dial on Lost Carrier

If the PPP connection is lost when auto-dial is used, the CMC will re-establish it automatically, helping to ensure seamless connectivity, by dealing with unreliable networks or “brown-outs” in coverage.

Dial-Up Configuration Management

The CMC allows the configuration of default dial-up connections to use for PPP connections and also the ability to specify if one or more dial-up connections are to activate the CDMA2000 PDSN connectivity feature.

WLAN Hotspot Access

In many WLAN hotspots, it is necessary to perform a web-login through a web-portal to gain general Internet access. With a mobile node enabled, where mandatory tunneling is enabled by default, it would not be possible to log in with the mobile node active because no traffic would be routed locally to the web-portal. Typically, this would require the mobile node to be disabled, breaking any active mobility sessions. The CMC overcomes this restriction by allowing HTTP and DNS access on the local interface, if the CMC determines that it has some network connectivity (obtains an IP address) but cannot access its home agent. This allows the user to log into the web-portal, and after successful login, the CMC will register with the home agent, and local HTTP/DNS access will be blocked (assuming mandatory reverse tunneling is employed). This feature provides for passage through WLAN web-portals at hotspots without breaking the mobility paradigm and tearing down Mobile IP sessions.

When a client changes the wireless link, the client sends a registration request to the home agent to register its new location. In public wireless LAN hotspots, there is a requirement to authenticate the end-user through a web page. Due to this requirement, the driver is actually opened up for network traffic outside the Mobile IP tunnel to allow this scenario. The driver will be closed for this side-traffic once the registration reply arrives.

Connectivity Support

The CMC can operate over any interface that appears as Ethernet (for example, LAN and WLAN) or PPP (dial, GPRS, UMTS) and can be installed and used on the target platform. The CMC will automatically detect the presence of the interface and, unless configured otherwise, will make it available for mobility usage.

Client Configuration and Profile Management

GUI Interface

CMC has a standard Graphical User Interface (GUI) that allows the user to configure the client.

Support for Multiple User Profiles

CMC user profiles contain the user configuration settings, keys, IP addresses, and rules regarding access, that determine the behavior of the CMC for the user. The profiles can be created using the GUI on the client. Profiles can also be created in an external tool, such as a text editor, and loaded into the CMC. The format is an XML-like structure. The CMC supports multiple loaded profiles, with easy switching to different profiles as needed. Switching to a new profile will shift to a new user identity, allowing the CMC to connect in a new topological manner. This is useful for consultants or other workers who need secure connectivity to different networks, from different places at different times, without having access to all simultaneously.

Multiple Users on the Same Device

As indicated in relation to user profiles above, multiple profiles can be installed. In addition, multiple users in Windows will have their own profiles. Therefore, a single PC can be shared between multiple Windows users and each will have their own CMC identities.

Flexible User Profile Installation Options

User profiles can be distributed and installed using a variety of methods. These include, downloading securely from the Cisco Home Agent, loading from a local file, automatic installation by clicking on a profile file (which may have been emailed or is on a CD), and it will be automatically installed on a running CMC. These mechanisms provide for simple adaptation of corporate IT policies.

Device Mode: One Profile for Multiple Users

Device mode is a method that allows a network administrator to easily configure the CMC so that all users of the device can use the same profile. Only the network administrator can change the settings and the functionality is transparent to the end user.

Log Viewer

A log viewer is included that allows users to view events of the CMC. This functionality is useful where checking is required when connectivity is not possible. The CMC log can be copied elsewhere and viewed by a support engineer.

The information displayed in the log includes the severity of the event, the time that the event occurred, and a brief description of the event. Clicking on a specific entry will allow users to view more details about the entry.

Software OS Support

Windows XP

The CMC supports Windows XP. It is also expected to a work with Windows XP Home, and the Tablet PC Edition.

Windows 2000

The CMC supports Windows 2000 included with the latest service pack 2 or later.

SEAMLESS ROAMING BASED ON STANDARD MOBILE IP (RFC 3344)

Basic Mobile IP Features

Standards-Based Mobile IP Support

The CMC supports IETF RFC 3344.

Mobile IP Reverse Tunneling

This feature allows tunneling of traffic from the mobile node to the home agent.

Mobile IP Standalone Foreign Agent Support

This feature supports communication with the home agent through a foreign agent where the Care-of Address (CoA) provided by the foreign agent is used in the Mobile IP registration.

Static Co-located Care-of Address Support

Supports communication with the home agent when no foreign agent is present using a Co-located Care-of Address (CCoA). In this case, the CMC will use a locally routable address as the CoA for the MIP traffic.

Dynamic Co-located Care-of Address Support

The CMC supports dynamic CCoA (the dynamic CCoA is similar to the CCoA above). If DHCP is provided on a remote network from where the CMC is establishing registration, then the DHCP assigned IP address is used as the CoA. If no DHCP IP address is provided, then a pre-configured static IP address can be used as the CoA. This feature is configurable by using the CMC GUI.

Dynamic Mobile Node IP Address Assignment

In this case, the CMC will use DHCP (with the Network Access Identifier (NAI) as a client identifier option) to obtain a dynamic IP address when it is at home. When it is away, the home agent will interact with the DHCP server to ensure the assignment of the same IP address, if it is already leased to the user. When it is away/collocated 0.0.0.0 is sent in registration requests indicating to the home agent that it needs to assign an IP address.

Advanced Mobile IP Features

Support for RFC 3519 NAT Traversal

The CMC provides full support for IETF RFC 3519 allowing access from remote locations to the home network where NATs or NAPTs occur between the mobile node and the home agent.

Mobile IP NAI Authentication

Support is provided for the use of the NAI for authentication and identification of the user when connecting to the network. The NAI is used in dynamic IP assignment but can also provide an identifier for user authentication.

Co-located Registration on the Intranet

This feature enables use of the internal IP address of the home agent when the Mobile Client is inside the intranet. Using an advertised identifier (such as a domain suffix) received in the DHCP assignment, the Mobile Client determines that it is on the intranet, but cannot directly access its home agent (no advertisement). In this case, it will attempt a co-located registration towards the internal IP address of the home agent (on the home network).

Public/Private Identification of the Home Agent

To allow mobility between the intranet and Internet, and access from outside the intranet, home agents are configured with public and private IP addresses. In the case of remote access, not on the home network, the public IP address is used as the destination for registration requests. When inside the home agent, a private IP address is used for de-registration requests. The use of two IP addresses allows for the placement of the home agent at the edge of the corporate network, supporting both external and internal access.

Passthrough Mode

This mechanism allows the CMC to communicate on a known network where it cannot access the home agent directly or through a foreign agent, and co-located connectivity is not preferred. With this mode of operation, the CMC will use a DHCP advertised item (for example, the domain suffix) to indicate that it is on an intranet network. In this case, the CMC will attempt a de-registration with the internal IP address of the home agent. If it succeeds, the CMC detects it in the intranet, and all traffic is allowed to go out on the physical adapters. While breaking the session continuity, as the IP address changes, it allows continued network access, in situations where mobility is not preferred. During this time, the CMC will continue to monitor for advertisements from home agent/foreign agent and enable mobility if the connectivity situation changes. This mechanism provides for deployment of mobility in certain circumstances in an Enterprise, without introducing triangular routing and excessive tunneling where it is not wanted. In passthrough mode, all traffic is handled by the operating system. There is no interference by the client software.

Interoperability with the Cisco Mobile IP Infrastructure

Cisco Mobile Client is interoperable with the Cisco IOS Home Agent Router, including Cisco 1800, 2800, 3800, and 7200 Series Routers.

Cisco Mobile Client is interoperable with the Cisco IOS Foreign Agent Router, including Cisco 1800, 2800, 3800, 7200 Series Routers, as well as the Cisco Mobile Access Router 3200.

SECURE MOBILITY

CiscoVPN client interaction

CMC supports the ability to automatically start the Cisco VPN client.

Compatibility with the Cisco Security Infrastructure

The Cisco Mobile Client when combined with the Cisco VPN Client provides a mobile VPN solution that is compatible with the Cisco VPN concentrators such as Cisco IOS Routers, Cisco 3000 Series Concentrators, Cisco ASA 5500 Series devices, and Cisco PIX Firewalls.

CMC is compatible with Cisco Secure Agent and Cisco Trust Agent.

Additional Features for Client Software Security

Lock-Down Mode

Lock-down support allows the administrator to restrict what options are available to the user in terms of CMC interaction. For example, the user can be restricted from disabling/stopping the CMC. This restriction would ensure that while the PC is on, all user traffic is tunneled to the Enterprise network, thereby limiting possibilities of security breaches, as all network traffic passes corporate firewalls/AV servers.

Mobile Client Password Protection

Depending on the deployment model, the CMC can request a user password at startup or not. In situations where the CMC is deployed, with a single user per PC, and where a Windows domain is employed, it may be regarded as unnecessary to have this login. This is an administrative issue configurable in the CMC profile.

Third-Party VPN Support

Third-party VPN clients are treated as separate applications and are expected to work correctly. No testing has been done with third-party clients.

INSTALLATION REQUIREMENTS

For Windows 2000 or XP

The Cisco Mobile Client, when installed on Windows 2000 or XP requires:

- Windows installation with a minimum of 128 MB RAM
- 5 MB free space on the hard disk
- Service pack 2 or later for Windows 2000
- No service pack dependencies for Windows XP

NIC Requirements

The Cisco Mobile Client is interoperable with any WLAN card supporting NDIS 5.1.

The Cisco Mobile Client interacts through PPP when interacting with GPRS and cdma2000 access cards; all PPP compatible cards are expected to work.

Table 1. Cisco IOS Home Agent Hardware and Software Requirements

Platform Support	Cisco IOS Software
Cisco 1700 Series Router	Cisco IOS Software Release 12.3(8)T
Cisco 1800 Series Router	Release 12.3(8)T
Cisco 2600XM Series Router	Release 12.3(8)T
Cisco 2800 Series Router	Release 12.3(8)T
Cisco 3600 Series Router	Release 12.3(8)T
Cisco 3700 Series Router	Release 12.3(8)T
Cisco 3800 Series Router	Release 12.3(8)T
Cisco 7200 Series Router	Release 12.3(8)T
Cisco 7300 Series Router	Release 12.3(8)T
Cisco 7400 Series Router	Release 12.3(8)T

Table 2. Cisco IOS Foreign Agent Hardware and Software Requirements

Platform Support	Cisco IOS Software
Cisco 1700 Series Router	Release 12.3(8)T
Cisco 1800 Series Router	Release 12.3(8)T
Cisco 2600XM Series Router	Release 12.3(8)T
Cisco 3600 Series Router	Release 12.3(8)T
Cisco 2800 Series Router	Release 12.3(8)T
Cisco 3200 Series Router	Release 12.3(8)T
Cisco 3700 Series Router	Release 12.3(8)T
Cisco 3800 Series Router	Release 12.3(8)T
Cisco 7200 Series Router	Release 12.3(8)T
Cisco 7300 Series Router	Release 12.3(8)T
Cisco 7400 Series Router	Release 12.3(8)T

STANDARDS COMPLIANCE

IETF RFC Compliance

Mobile IP

- **RFC 2003**—IP-IP Encapsulation
- **RFC 2005**—Applicability Statement for IP Mobility Support
- **RFC 2085**—HMAC-MD5 IP Authentication with Replay Prevention
- **RFC 2104**—HMAC: Keyed-Hashing for Message Authentication
- **RFC 2486**—The Network Access Identifier
- **RFC 3012**—MIPv4 Challenge/Response Extensions
- **RFC 3024**—Reverse Tunneling for Mobile IP, revised
- **RFC 3115**—MIP Vendor Extensions
- **RFC 3344**—IP Mobility Support for IPv4, revised
- **RFC 2794**—MIP NAI Extension
- **RFC 3519**—Mobile IP Traversal of Network Address Translation (NAT) Devices

Dynamic Host Configuration Protocol

- **RFC 2131**—Dynamic Host Configuration Protocol
- **RFC 2132**—DHCP Options and BOOTP Vendor Extensions

3GPP2 cdma2000 Compliance

TIA-835 cdma2000 Release B Wireless IP Standard

- Dynamic MN-IP Address Assignment
- RADIUS MN-AAA Authentication

ORDERING INFORMATION

Where to Buy Cisco Products

- http://www.cisco.com/public/ordering_info.shtml

Product and Part Numbers

Cisco Mobile Client is a companion of Cisco IP Mobility Gateway Feature license. The client can be downloaded at: http://www.cisco.com/cgi-bin/tablebuild.pl/cmc-1.0

The IP Mobility Gateway Feature license part numbers are listed below and can be ordered through the ordering link at: http://www.cisco.com/public/ordering_info.shtml

Table 3. Part numbers for the Cisco IOS Mobility Gateway (Home Agent) Feature license

Description	Part Number
IP Mobility Gateway Feature Set—up to 100 Users	FL-IPMOBGW-100=
IP Mobility Gateway Feature Set—up to 500 Users	FL-IPMOBGW-500=
IP Mobility Gateway Feature Set—up to 1000 Users	FL-IPMOBGW-1000=

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 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 the USA 206634.F_PI_04/06