

Cisco Prime Access Registrar

Product Overview

Cisco Prime™ Access Registrar is a carrier-class solution that provides scalable, flexible, intelligent authentication, authorization, and accounting (AAA) services.

Service providers face tremendous challenges in deploying and managing mission-critical access services.

These include:

- Efficiently serving an increasingly diverse mix of access technologies (and corresponding authentication protocols), users, and roaming partners
- Rapidly delivering new subscriber services for competitive advantage (for example, a new prepaid service)
- Facilitating different service delivery models such as mobile virtual network operators (MVNOs)/wholesale and roaming
- Efficiently managing resources like IP addresses or session limits
- Keeping up with scalability demands

Adding to this complexity is the fact that many service providers have multivendor, heterogeneous AAA environments and increasingly complex business requirements. Service providers also are under pressure to reduce operating expenses (OpEx) and have to keep up with the need to centralize data stores and adapt billing systems. Operators need a comprehensive access management solution to address these issues.

In addition, given today's explosive mobile data growth, network operators are often finding that third-generation (3G) networks are not equipped to handle the load on the network, and one key problem relates to signaling. Today's smartphones include applications that can request data from the network every few minutes, and this number of radio authentication requests can easily overwhelm the radio access and core network elements involved with authentication, encryption, and billing systems. As a result, mobile operators face the prospect of needing to continually increase the capacity of network equipment.

Wi-Fi appeals to many operators as a cost-effective means of offloading large amounts of mobile data traffic while delivering a variety of new services. It offers these features:

- Widespread existing deployments
- Availability of user devices that support the technology
- Cost efficiency
- Capability to address new users and devices without mobile subscription (without a Subscriber Identity Module [SIM])
- Globally available spectrum capacity
- Standards availability for integration into mobile core networks

Operators need an AAA solution that can support this Wi-Fi offload capability.

Cisco Prime Access Registrar provides a 3GPP-compliant RADIUS/Diameter server designed from the ground up for scalability and extensibility for deployment in complex service provider environments including integration with external data stores and systems and multivendor network access servers (NASs). Session and resource management tools track user sessions and allocate dynamic resources to support new subscriber service introductions. The solution supports service provider deployment of access services by centralizing AAA information and simplifying provisioning and management.

Cisco Prime Access Registrar Director provides proxy function and scripting capability for RADIUS. Cisco Prime Access Registrar Director is intended for use in scenarios such as roaming or those in which a customer is going to use the solution to perform an intelligent proxy or load-balance the RADIUS packet based on certain conditions or rules.

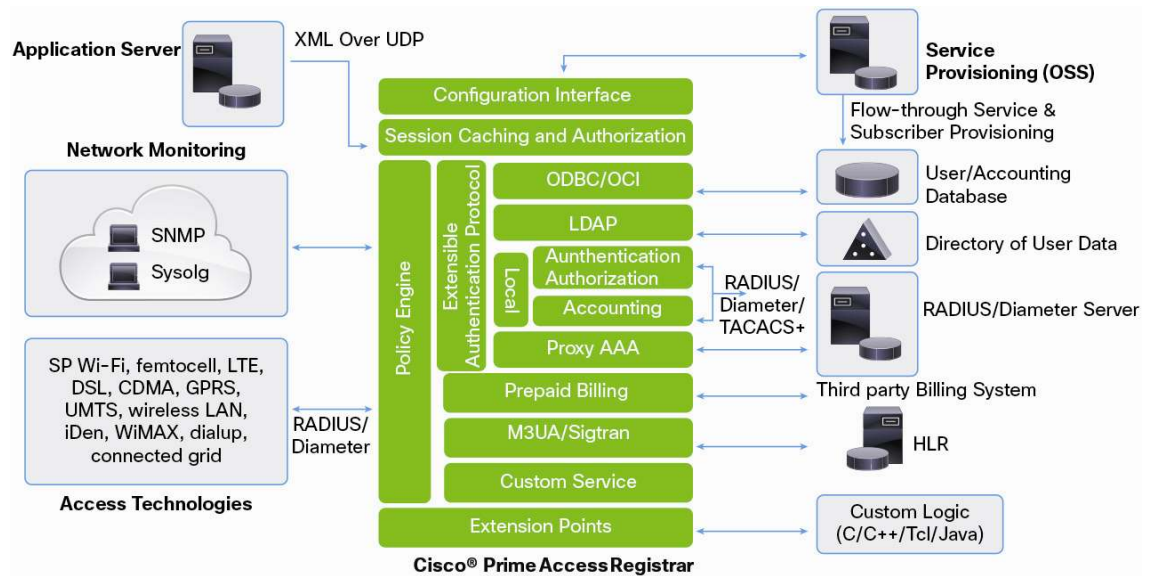
Product Architecture

At the core of Cisco Prime Access Registrar (Figure 1) is a policy engine that determines processing based on the contents of the request packet. The policy engine makes the following types of decisions:

- Whether to perform one or more of the following against any incoming packet: authentication, authorization, accounting, proxy.
- Which authentication/authorization data store to perform authentication and authorization against: Supported options are Lightweight Directory Access Protocol Version 3 (LDAPv3) directories (including Microsoft Active Directory [AD]), Oracle database, MySQL database, and the local embedded database.
- What type of authentication to use: Built-in authentication mechanisms or a custom-built mechanism. Built-in mechanisms include Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and the following Extensible Authentication Protocol (EAP) authentication methods: EAP-SIM/AKA/AKA-PRIME (AKA') over M3UA/SIGTRAN and SWx (Diameter), EAP-TLS, EAP-TTLS, EAP-GTC, EAP-MSCHAPV2, LEAP, EAP-FAST, EAP-MD5, PEAPv0, and PEAPv1.
- Whether accounting against an external database like Oracle or MySQL or a local flat file is required.
- Whether a request should be proxied to an external RADIUS/Diameter server.
- What type of accounting is required.
- Whether user/group session limits apply.
- Whether an IP address has to be allocated and whether to use static mapping or to allocate one from a preconfigured pool.

While the basic operation of the server is determined by configuration, multiple extension points within the server provide optional callouts to custom code. Extension points can be used for several purposes, including influencing the processing of a request or modifying incoming or outgoing packets to meet specialized requirements.

Figure 1. Cisco Prime Access Registrar Architecture



Features and Benefits

- Supports a broad range of wireless and wireline **access technologies** on a common AAA server platform, delivering operational and capital expense savings while providing flexibility to the service provider regarding choice in AAA.
- Provides extensive **subscriber data store** support including an internal database and integration with external databases including Oracle, MySQL, Microsoft AD, and OpenLDAP through the use of connectivity mechanisms such as Open Database Connectivity (ODBC), LDAP, Oracle Call Interface (OCI), and Java Database Connectivity (JDBC).
- Provides **scalability** to support large service deployments. An external session manager allows tens of millions of simultaneous active sessions. Additionally, the multithreaded architecture provides performance that scales with additional CPUs.
- Efficiently **manages resource use** with real-time session management to track user sessions and dynamically allocate resources like IP addresses and user/group session limits.
- Gives service providers an off-the-shelf, standards-based RADIUS/Diameter server that is highly **flexible and extensible**. With extension point scripting (EPS), the solution can be customized to meet unique business, regulatory, and technical requirements.
- Provides broad **integration support**: Reduces operational costs and speeds service rollout by supporting integration with provisioning, billing, and other service-management components.
- Supports seamless Wi-Fi data offload through the ability to interface directly with the Home Location Register (HLR) through an M3UA/SIGTRAN interconnectivity layer or Home Subscriber Server (HSS) through the Wx interface over Diameter.

Table 1 lists detailed features and benefits of Cisco Prime Access Registrar.

Table 1. Features and Benefits

Feature	Benefit
Access Technology Support	
Support for a broad range of wireless and wireline access technologies, including Service Provider Wi-Fi (SP Wi-Fi), femtocell, LTE, DSL, Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), Universal Mobile Telecommunications Service (UMTS), wireless LAN (WLAN), iDen, WiMAX, dialup, Connected Grid, and others.	By helping enable standardization on a common AAA server platform complying to appropriate 3GPP AAA standards, the solution delivers operational and capital expense savings while providing flexibility to the service provider regarding choice in AAA.
Support for femtocell network rollouts in conjunction with Cisco Prime Cable Provisioning and Cisco Prime Network Registrar. Cisco Prime Access Registrar acts as the RADIUS headend to authenticate and authorize a 3G femtocell.	Extends AAA resources where they may already be deployed. For a mobile operator, femtocells provide improvements to both coverage and capacity, especially indoors where access would otherwise be limited or unavailable. Consumers benefit from improved coverage and potentially better voice quality and battery life.
Identity and access management for Cisco® Connected Grid solutions on IPv6 networks. This is achieved using the Elliptic Curve Cryptographic (ECC)-based certificate validation and also supports TACACS+ authentication, command authorization, and accounting. For EAP services, in addition to RSA certificates, the solution supports verification of ECC certificates. ECC uses elliptic curves to encrypt data when creating keys, which enables creation of shorter and stronger keys for better efficiency. This is achieved using the Cisco SSL library APIs.	Provides high performance AAA support for authenticating smart meters on a Connected Grid network. Allows granular control of device/user administration of pole top routers through TACACS+ authentication.
Authentication and Authorization	
High-speed internal embedded user database	<ul style="list-style-type: none"> • Provides a rapid start point for small-scale deployments • Allows easy, logical grouping of users • Offers easy configuration to return attributes in responses and check attributes ("check items") in requests • Provides operator ability to enable and disable user access
Ability to authenticate/authorize user information stored in an external data store: LDAP directory (like Microsoft AD, OpenLDAP), Oracle or MySQL database, combined with the ability to: <ul style="list-style-type: none"> • Store return and check-items attributes • Add custom logic based on information in user's record 	Integration support is data-store schema independent, simplifying deployment and day-to-day operations, providing OpEx savings by using existing infrastructure, and helping to support networks with tens of millions of subscribers.
Advanced RADIUS/Diameter proxy support for service provider environments <ul style="list-style-type: none"> • Includes ability to add/modify/delete attributes while proxying attributes 	Facilitates roaming arrangements with other service providers and load balancing.
Rich set of authentication protocols including support for EAP-proxy and certificate revocation list (CRL) <ul style="list-style-type: none"> • PAP, CHAP, MSCHAPv2, LEAP, PEAPv0, PEAPv1 • EAP-MD5, GTC, EAP-FAST, EAP-TLS, EAP-TTLS • EAP-SIM/AKA/AKA' to authenticate with HLR over M3UA/SIGTRAN or HSS over SWx (Diameter) • EAP Negotiate (run-time selection of EAP service) • EAP proxy • Diameter NASREQ • HTTP Digest Authentication • LDAP remote server bind-based authentication • CRL support for EAP services 	Broad user support with the ability to extend to others such as POP3 through custom services for meeting unique requirements.
EAP-SIM authentication from an EAP-AKA or EAP-AKA' source (quintets to triplets conversion)	Provides backward compatibility.
IETF RADIUS tunnel support	Provides support for VPN authentication.
Automatic and customizable reply-message generation	Helps provide detailed information in case of authentication rejects.

Feature	Benefit
Accounting	
Local file <ul style="list-style-type: none"> Ability to store accounting records in a single file or multiple files Automatic file rollover based on file age, size, or specific time 	Speeds up processing through the ability to store accounting information on the same server on which the AAA services are running.
Proxy <ul style="list-style-type: none"> Option to ignore acknowledgements and continue processing 	Accelerates decision-making logic when responses (or lack of) from certain remote systems can be ignored.
Database/LDAP <ul style="list-style-type: none"> Ability to write accounting records directly to an Oracle or MySQL database or an LDAPv3 directory Buffering option for relational database management systems (RDBMSs) for higher throughput and fault tolerance 	Integration support is schema independent, simplifying deployment and day-to-day operations, providing OpEx savings by using existing infrastructure, and helping to support networks with tens of millions of subscribers.
Option to have a mix of multiple types of accounting (local file, proxy, database) and destinations within each type.	Provides flexibility and customer choice.
Platform Support	
Supported operating systems: <ul style="list-style-type: none"> Oracle Solaris 10¹ Red Hat Enterprise Linux (RHEL) 5.3, 5.4, 5.5, 6.0, 6.1, and 6.2 	Broad operating system support for customer choice.
Support for virtualization technologies: Oracle VM Server for SPARC and VMware ESXi 5.0	Lowers total cost of ownership (TCO), eases deployment, and provides greater flexibility in migration and backup.
Various Technology Support	
IPv6 support: <ul style="list-style-type: none"> Performs processing of RADIUS/Diameter requests from IPv6 RADIUS/Diameter clients/servers Proxies requests to and receives responses from a remote IPv6 RADIUS/Diameter server Interacts with external database servers using IPv6, including LDAP, Oracle, and MySQL Allows HTTP and Simple Network Management Protocol (SNMP) to be queried over IPv6 	Provides support for IPv6 networks and dual-stack IPv4/IPv6 networks.
Diameter support	Provides the following facilities: <ul style="list-style-type: none"> Supports authentication and authorization of Diameter packets with the help of a local database or an external database with interfaces such as LDAP and ODBC Performs session management and resource management Supports writing a Diameter accounting packet in a local file or proxying to another AAA server Supports adding, modifying, or deleting the attribute-value pairs (AVPs) in Diameter packets through extension point scripting Supports open-ended Diameter applications Supports translation of incoming RADIUS requests and responses to Diameter and vice versa
Compliance with the WiMAX Network Working Group (NWG) stage 3 document version 1.3.1.	Meets the various WiMAX NWG requirements for WiMAX networks.
Support for SP Wi-Fi/hotspot markets and wireless data offload including: <ul style="list-style-type: none"> Wx interface support for HSS lookup: Cisco Prime Access Registrar supports SIM and Universal SIM (USIM) authentication for data access against the newer generation subscriber database HSS through the Diameter interface Wx Cisco Prime Access Registrar also provides authentication support against the Home Location Register and external databases including Oracle, MySQL, OpenLDAP, and AD M3UA/SIGTRAN interface to HLR server on Linux operating systems for providing seamless Wi-Fi data offload services using SIM and USIM authentication 	Helps enable service providers to effectively provide SP Wi-Fi and wireless data offload functionality.

Feature	Benefit
Proxy, Database, and LDAP Configuration	
<p>Remote server support:</p> <ul style="list-style-type: none"> Operator is able to define a list of remote systems to be used in failover or round-robin modes Operator is able to define the individual characteristics of each remote system, for example, ports, timeouts, retries, or reactivate timers Sophisticated algorithms detect status of remote systems 	Provides option to perform authentication, authorization, and accounting against a wide variety of remote systems with adequate options for load balancing and handling failure scenarios.
<p>Outage policies: When no remote systems are available, Accept All, Reject All, and Drop Packet outage policies are available.</p>	Helps enable AAA processing to occur based on preconfigured policies even when remote systems are not available.
Rule and Policy Engine for Decision Making	
<ul style="list-style-type: none"> Ability to process requests using different types of data stores; for example, use LDAP for some access requests, the internal database for others Ability to process requests using a variety of options; for example, store an accounting request to a local file and proxy it to a number of remote RADIUS/Diameter servers, in series or in parallel, waiting for acknowledgement from some and not from others Ability to split authentication and authorization by selecting one method for authentication and another for authorization (One-Time Password [OTP] server and Oracle database, for example) Ability to decide how to process a packet based on attributes in the request packet such as source or destination IP address or User Datagram Protocol (UDP) port or based on Cisco Prime Access Registrar's environment variables settings such as reauthentication service, reauthorization service, and reaccounting service Easy request processing options based on a variety of attributes/values like DNS domain, username prefix, dialed number, calling number, NAS, and others, using the predefined policies in Cisco Prime Access Registrar policy engine 	Provides a variety of predefined rules and policies for meeting most usual requirements in service provider environments. Provides the ability to extend default logic with custom policies written using C/C++/Tool Command Language [Tcl]/Java.
<p>Flexible AAA processing through use of logical operators</p>	<p>Logical operators AND, OR, PARALLEL-AND, PARALLEL-OR provide extreme flexibility in evaluating AAA processing choices in serial or parallel. Parallel is used when a response from any one subsystem is sufficient to trigger a decision process and also helps reducing processing time. Serial is used when a sequential response from subsystems is required.</p>
<p>Simplified GUI/CLI mechanism to easily choose the right authentication, authorization, and accounting service(s) required for processing a packet.</p>	<ul style="list-style-type: none"> Provides maximum flexibility and ease in matching information in the incoming packets for choosing the appropriate service to apply Provides a very simple method to add, modify, or delete AVPs in packets Reduces the need for scripting or requirement of familiarity with programming languages such as TCL, C, C++, or Java Provides easy and efficient alternative to rule/policy engine and scripting points for most common use cases
Session Management and Resource Allocation	
<p>Built-in feature to track user sessions</p>	
<p>Dynamic resource allocation including:</p> <ul style="list-style-type: none"> Session limits IP addresses 	<p>Supports:</p> <ul style="list-style-type: none"> Enforcement of session limits per user and per group Allocation of critical resources such as IP-addresses and home-agents
<p>Options to store active session information to an external database like Oracle</p>	Helps enables scaling up to tens of millions of sessions per server.
<p>In an environment with multiple Cisco Prime Access Registrar servers, the operator may designate one Cisco Prime Access Registrar to manage all sessions</p>	Helps avoid bypass of session limits and to allocate IP addresses and other resources centrally.
<p>Session query capabilities:</p> <ul style="list-style-type: none"> Real-time query of the session table using the command-line interface (CLI), XML over UDP, RADIUS, or Diameter Able to query cached attributes through the query session Able to query and release sessions based on session age, username, NAS, and other criteria 	Allows external/business applications to query Access Registrar for information on users who are logged in and the resources (like IP-address) that they are allocated. This can then be used for making other business decisions such as providing personalized services, reduced sign-on, and enhanced video delivery.

Feature	Benefit
Session release capabilities: <ul style="list-style-type: none"> • Manual release of sessions and resources • Automatic session release when accounting stop is lost (inactivity timeout) • Able to release sessions and generate Packet of Disconnect (PoD) • Automatic session release when accounting on/off is detected (system accounting) 	Helps manage session state information across the network automatically or through administration intervention.
Session information not lost even if Cisco Prime Access Registrar or the system is restarted	Avoids information loss during server restarts that can otherwise wreck user/group session limit enforcement or allocation of IP addresses.
Session tracking for accounting-only servers: Able to count the number of user sessions	Session management can be done for servers through which only accounting messages pass through. This can be used in cases such as username to IP address resolution or International Mobile Subscriber Identity (IMSI) to IP address resolution where only accounting traffic is forwarded through Cisco Prime Access Registrar.
Ability to send Change of Authorization (CoA) request	Helps in changing service levels of users who are logged in, on the fly. For example, a user on a 1 MB plan could be bumped up to 2 MB without having to log off.
Scalability	
An external session manager allows tens of millions of simultaneous active sessions by storing the active session records on an external database server (Oracle10g and 11i) instead of storing them in the internal memory of Cisco Access Registrar	Supports large service deployments with a single instance of Cisco Prime Access Registrar.
Multithreaded architecture provides performance that scales with additional CPUs	Supports large service deployments with a single instance of Cisco Prime Access Registrar and allows the solution to grow with the business.
Customization/Extensibility	
Ability to add custom logic to the request processing flow using Tcl, C or C++, or Java through extension point scripting: <ul style="list-style-type: none"> • Access request and response packets • Modify processing decisions in real time • Target specific requests with multiple callout points • Add, delete, or modify the AVPs EPS allows users to interact with request processing and communicate with Cisco Prime Access Registrar at numerous API points	Helps enable meeting unique business, regulatory, and technical requirements.
Able to create custom processing methods	Helps to meet new/unique business requirements. For example, custom code can be written and integrated to support authentication mechanisms, such as POP3, which are not built into Cisco Prime Access Registrar.
Extensible attribute dictionary <ul style="list-style-type: none"> • Populated with latest attribute definitions, including third-party, vendor-specific attributes • Easy addition of new attributes (add/modify/delete) • Variable-length vendor type in vendor-specific attributes 	Easy interoperability with third-party devices.
Resilience	
<ul style="list-style-type: none"> • Automatic configuration replication to other Cisco Prime Access Registrar servers • Specify lists of alternate remote systems for each processing method • Specify multiple methods to process a request • Automatic server restart 	Provides multiple levels of redundancy including server redundancy, remote-system redundancy, and processing-method redundancy.
Veritas, Sun, and Red Hat Enterprise Linux (RHEL) clustering for high availability	Minimizes application downtime.

Feature	Benefit
Troubleshooting and Monitoring	
Multilevel debugging output	Helps troubleshoot and isolate incidents faster. Allows controlling error, debug output.
Statistics: <ul style="list-style-type: none"> Real-time query of statistics Reset statistics without restarting Cisco Prime Access Registrar 	Statistics are provided for a variety of events occurring within the server, such as number of packets processed, number of packets dropped, number of packets proxied to remote server, received response, and so on. These help in analyzing usage patterns, troubleshoot issues, and more.
Able to query status of all Cisco Prime Access Registrar processes and utilities	Offers simple utilities that show status of all Cisco Prime Access Registrar-related processes to help in troubleshooting.
Logging: <ul style="list-style-type: none"> Log files for each Cisco Prime Access Registrar process Audit log of all configuration changes Able to direct logs to a syslog server 	Provides multiple logs for various components and logging levels that help manage and isolate incidents quicker. Provides audit trails that can be maintained through configuration change logs.
SNMP: <ul style="list-style-type: none"> RADIUS SNMP support SNMP traps generated for critical events 	Allows for easy monitoring from network management systems.
Utility to generate RADIUS AAA requests: Radclient	Helps to simulate network deployment scenarios in a lab through: <ul style="list-style-type: none"> Creation of individual packets of various types - access-requests, accounting requests, and more. Simulating stress/performance testing scenarios to exhibit server behavior and for tuning the system
Configuration	
<ul style="list-style-type: none"> Powerful command-line configuration utility with interactive/noninteractive full and view-only modes Dynamic configuration feature allows configuration changes to take effect without a server restart Command and value recall, inline editing, autocommand completion, and a context-sensitive list of options Revamped web-based interface for configuring most of the objects in Cisco Prime Access Registrar Wildcard definitions for grouping RADIUS clients 	Noninteractive modes allow for configuration automation and OSS integration. Powerful CLI allows easy interactive operations saving operators time and helping avoiding errors.
Broad Systems Integration Capabilities	
Support for integration with provisioning, billing, and other service-management components	Reduces operational costs and speeds service rollout.
Prepaid billing interface allows billing vendors to integrate their systems into Cisco Prime Access Registrar for prepaid functionality	Service providers may offer prepaid data or usage-based premium services while reusing their existing billing system and protecting their investments.
Management	
<ul style="list-style-type: none"> Replication of the internal databases allows multiple servers to be similarly configured Supports SNMP and syslog for network management 	Centralized management and ease of use.

System Requirements

Table 2 lists system requirements for Cisco Prime Access Registrar 6.1.

Table 2. Server System Requirements

Server Requirements		
Operating system	Solaris 10 [*]	Linux RHEL 6.2
Model	SPARC Enterprise T5220	X86
CPU type	UltraSPARC-T2 (SPARC V9)	Intel® Xeon® Processor E5-2630
CPU number	8 cores (8 threads each)	6 cores (12 Threads each)
CPU speed	1165 MHz	2.30GHz

Server Requirements		
Memory (RAM)	8 GB	8 GB
Swap space	10 GB	10 GB
Disk space	2 x 72 GB	1 x 146 GB

*Solaris support is available for Cisco Prime Access Registrar Version 6.0. Solaris support for Version 6.1 will be provided in a future maintenance release.

Ordering Information

To place an order, visit the [Cisco Ordering Homepage](#). To download software, visit the [Cisco Software Center](#).

About Cisco Prime

The Cisco Prime portfolio of enterprise and service provider management offerings empowers IT organizations to more effectively manage their networks and the services they deliver. Built on a service-centered foundation, Cisco Prime supports integrated lifecycle management through an intuitive workflow-oriented user experience, providing A-to-Z management for IP next-generation networks, mobility, video, cloud, and managed services.

Cisco Services

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

For More Information

For more information about Cisco Prime Access Registrar, visit <http://www.cisco.com/go/accessregistrar>, contact your local account representative, or send an email to ar-tme@cisco.com for presales/business queries or cs-ar@cisco.com for technical queries.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)