Cisco Access Registrar 5.0

High Performance Carrier Class RADIUS/Diameter Solution

Product Overview

Cisco® Access Registrar (Cisco AR) is a high performance carrier class RADIUS and Diameter solution for access services. Cisco AR simplifies the deployment and management of access services, helping enable service providers to:

- **Accelerate deployment of access services:** Intelligent authentication, authorization, and accounting (AAA) services
- **Implement an "end-to-end" solution for multiple access technologies:** High performance, scalable, reliable, and flexible
- **Reduce operational costs:** Centralized management and simplified administration

Cisco Access Registrar 5.0 introduces a number of new features and enhancements that can benefit current and potential customers of Cisco Access Registrar.

Highlights

Diameter support

Cisco Access Registrar 5.0 adds support to the Diameter base protocol as per RFC 3588. The Diameter base application needs to be supported by all Diameter implementations.

Support for Diameter provides the following facilities:

- Supports authentication with the help of a local database or an external database (such as Lightweight Directory Access Protocol [LDAP], Open Database Connectivity [ODBC])
- Does session management and resource management as Cisco Access Registrar currently does for RADIUS packets
- Supports writing the Diameter accounting packet in a local file or proxy to another AAA server
- Supports adding, modifying, or deleting the attribute-value pairs (AVPs) in Diameter packets through extension point scripting only for the local AAA service
- Supports open-ended Diameter applications

Cisco Access Registrar 5.0 processes Diameter packets through profiles, polices, and rules, the same as for RADIUS packets, and supports session management and extension point scripting. Cisco Access Registrar 5.0 supports authentication through external databases with interfaces such as LDAP and ODBC.

Another application that is supported as a part of this release is the Diameter Network Access Server Application as per RFC 4005.

IPv6 interface support

Cisco Access Registrar 5.0 provides support for:

- Processing of RADIUS requests originated from an IPv6 RADIUS client (network access server [NAS])
- AAA proxy for remote IPv6 AAA server
- IPv6 or IPv4 as the interface between Cisco Access Registrar and Broadband Remote Access Server (BRAS)/NAS
- IPv6 as per RFC 3162 attributes

EAP-AKA support

Cisco Access Registrar 5.0 provides support for Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) as per RFC 4187.

The following EAP-AKA features are supported:

- MAP protocol
- Home Location Register (HLR) and Home Subscriber Server (HSS) and the list of compliant Third-Generation Partnership Project (3GPP) standards
- Messages exchanged with the HLR/HSS
- Description of the HLR/HSS
- User profile information

Cisco Access Registrar servers have support for migration to a converged IP next-generation network (IP NGN) by supporting SIGTRAN SS7 messaging over IP (SS7oIP) for HLR communication to facilitate the seamless transition to next-generation IP-based signaling networks.

SIGTRAN, a working group of the Internet Engineering Task Force (IETF), has defined a protocol for the transport of real-time signaling data over IP networks. Cisco Access Registrar supports SS7oIP through SIGTRAN, a new transport layer that uses Stream Control Transmission Protocol (SCTP).

WiMAX NWG stage 3 latest document support

The WiMAX forum keeps updating the stage 3 document to address various requirements needed in the WiMAX communication between various devices that exist in the network. Cisco Access Registrar 5.0 complies with the Network Working Group (NWG) stage 3 document version 1.3.1 released in 2009 and addresses the newly added WiMAX attributes.

WiMAX provisioning server support along with bootstrap encryption key

Cisco Access Registrar 5.0 provides support to generate and cache the bootstrap encryption key (BEK) when it receives the authentication request from the unprovisioned WiMAX subscriber or device.

Cisco Access Registrar can identify the unprovisioned device either by looking into the special pattern in the access request (for example, the User-Name attribute used in a RADIUS access request will be a temporary ID that indicates the unprovisioned device) or by performing explicit database lookup.

When the Cisco Access Registrar receives the accounting start packet for the unprovisioned device:

- IP, MAC address, and BEK of this unprovisioned device need to be sent to the Open Mobile Alliance Device Management (OMA-DM) server to initiate the provisioning
- Cisco Access Registrar needs to maintain the IP address to MAC address association using the web service until it receives the provisioning complete message from the OMA-DM server

The back-end portal could query the Cisco Access Registrar web service for this unprovisioned device MAC address by giving the device IP address and also the OMA-DM server request to the Cisco Access Registrar web service to validate the MAC to IP address association.

The communication between Cisco Access Registrar and OMA-DM/portal server is through the web service by using Simple Object Access Protocol (SOAP) over HTTPS. It is assumed that the OMA-DM server (or a mediation function) will have a web service that Cisco Access Registrar can use to communicate.

Lawful intercept support in Cisco Access Registrar

Cisco Access Registrar 5.0 provides support for Intercept Access Point (IAP), which is responsible for receiving the intercept/monitoring request for the subscriber whose Access Associated Communications Identifying Information (AA CMII) is to be intercepted and delivered to a Law Interception Server (LIS).

The following intercept requests from LIS are supported by Cisco Access Registrar 5.0:

- **ProvisionTarget:** To start monitoring the target user
- **DeprovisionTarget:** To stop monitoring the target user
- **LinkUpdate:** To query the target user in monitored list
- **ListTarget:** To list all the users that are currently being monitored

Session scalability

The goal is to enhance the current session scalability of Cisco Access Registrar to hold multimillions of active sessions by storing the active session records on an external database server (Oracle) instead of storing it in the internal memory of Cisco Access Registrar.

Some of the internal variables and data structures of session management are modified in such a way as not to affect existing functionality as well as to optimize database reads/writes by means of a cache.

With a single instance of Cisco Access Registrar 5.0, customers can scale multimillions of active sessions. Session scalability of Cisco Access Registrar with an external database depends upon the potentiality of the database. Supported Oracle database servers are 10g and 11i.

An option is provided to the customer to decide whether the active session information needs to be stored internally or externally.

Interim accounting update support for ODBC server

Cisco Access Registrar Release 5.0 will address the interim accounting records with DELETE and UPDATE entries to the external database.

LDAP accounting write-up

Cisco Access Registrar supports the LDAP interface for authentication and authorization. Cisco Access Registrar Release 5.0 will start support for LDAP write-up for accounting request messages to an external LDAP directory.

Red Hat Enterprise Linux 5.3 support

Considering the changing business needs of the customer, Cisco Access Registrar 5.0 has started supporting Red Hat Enterprise Linux (RHEL) 5.3.

GUI revamp

In Cisco Access Registrar Release 5.0 the graphical user interface (GUI) is completely revamped with the latest Java technologies to give a better look and feel with support for configuring most of the objects in Cisco Access Registrar. The Cisco Access Registrar 5.0 GUI has support for Internet Explorer versions 6, 7, and 8.

Support for Veritas clustering

Cisco Access Registrar 5.0 supports Veritas clustering. The Veritas Cluster Server is the industry's leading cross-platform clustering solution for minimizing application downtime. Through central management tools, automated failover features to test disaster recovery plans without disruption, and advanced failover management based on server capacity, Cluster Server allows IT managers to maximize resources by moving beyond reactive recovery to proactive management of application availability.

VMware support

Cisco Access Registrar Release 5.0 officially starts supporting VMware ESX for Linux machines.

VMware ESX is an enterprise-level virtualization product offered by VMware, Inc. ESX is a component of VMware's larger offering, VMware Infrastructure, which adds management and reliability services to the core server product.

UCS support

Cisco Access Registrar Release 5.0 supports Cisco’s Unified Computing System (UCS).

Cisco UCS represents a radical simplification of traditional architectures, dramatically reducing the number of devices that must be purchased, cabled, configured, powered, cooled, and secured. The solution delivers end-to-end optimization for virtualized environments while retaining the ability to support traditional OSs and application stacks in physical environments.

Cisco UCS is built to meet today's demands while being ready to accommodate future technologies - including more powerful processors and faster Ethernet standards - as they become available.

Cisco Access Registrar Director license

Cisco Access Registrar Director is a lightweight software version of Cisco Access Registrar that provides only the proxy function and scripting capability. Cisco Access Registrar Director can be used in proxy scenarios in which a customer is going to use Access Registrar only for the proxy functionality or in load balancing where Access Registrar can be used as a load balancer to the backed RADIUS servers. No other service is available as part of Cisco Access Registrar Director. It supports both RADIUS and Diameter proxies.

Benefits

Cisco Access Registrar provides the following benefits:

- Supports multiple access technologies (dial, wholesale dial, broadband, mobile wireless, wireless LAN and public wireless LAN, Service Selection Gateway [SSG], VoIP, cable, WiMAX) with a single AAA platform.
- Gives service providers an off-the-shelf, standards-based RADIUS/Diameter server that offers the flexibility and extensibility previously available only by maintaining internally built versions of public-domain RADIUS/Diameter software.
- Allows service providers to focus their businesses on specific areas of service delivery by supporting additional wholesale, outsourcing, and roaming service scenarios using proxy RADIUS/Diameter.
- Reduces operational costs and speeds service rollout by supporting integration with provisioning, billing, and other service-management components using directory or relational database management system (RDBMS) support and scriptable configuration interfaces.
- Efficiently manages resource use by supporting centralized IP address assignment and session-limit enforcement across access devices spanning multiple geographic regions and across multiple Cisco Access Registrar servers.
- Allows service providers to extend competitive advantages by rapidly deploying the latest wireless technologies.

- Provides multimillion session scalability by off-loading the active session information to an external database like Oracle.

Product Architecture

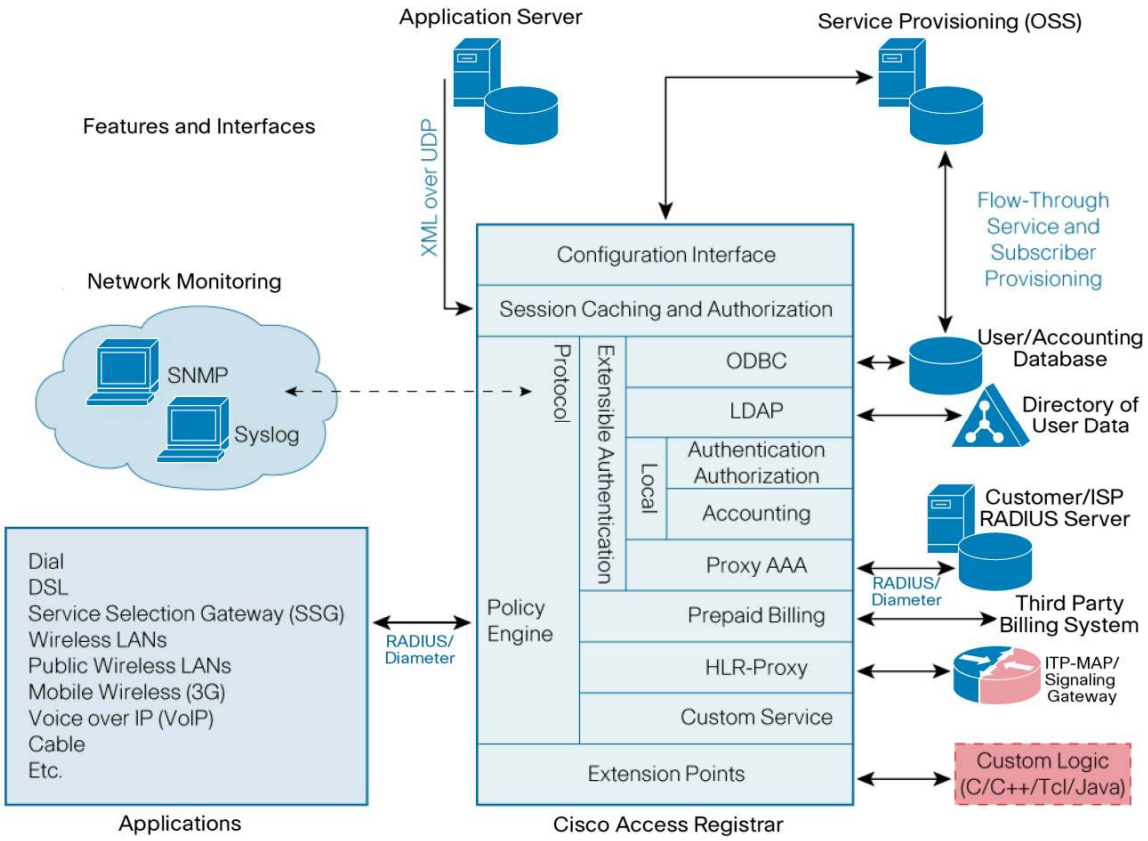
Cisco Access Registrar is built on a multithreaded architecture to take advantage of multiprocessor systems and provide the highest AAA performance. At the core of Cisco Access Registrar (Figure 1) is a policy engine that determines processing based on the contents of the RADIUS/Diameter request packet. The policy engine makes the following types of decisions:

- Whether authentication against an LDAP directory, Active Directory, or Oracle database is required
- Whether accounting against an LDAP directory or Oracle database is required
- Whether a request should be forwarded to an external RADIUS/Diameter server
- What type of accounting is required
- Whether session limits apply
- Whether an IP address pool has been assigned

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.

Cisco Access Registrar provides a rich set of processing methods, including local, LDAP, ODBC, Active Directory, proxy, and prepaid, but Cisco Access Registrar also permits custom service code to be inserted into its architecture to allow service providers to support special request processing and systems integration.

Figure 1. Cisco Access Registrar Architecture



Features

Authentication and Authorization

- High-speed internal embedded user database
- Easy, logical grouping of users
- Easy return attributes and check-item configuration
- Ability to enable and disable user access
- Ability to store user information in an external data store
- LDAP directory or Oracle or MySQL database support:
  - Store return and check-items attributes
  - Data store schema independent
  - Ability to add custom logic based on information in user's record
- Authentication to a Windows database Advanced RADIUS/Diameter proxy support for service provider environments
  - Includes proxy attributes filtering
- EAP support
  - Message Digest Algorithm 5 (MD5), LEAP, PEAP (with Microsoft Challenge Handshake Authentication Protocol [MS-CHAP]) version 2, Generic Token Card (GTC), SIM, TLS, FAST, TLS, TTLS, AKA
  - EAP proxy
  - EAP-Negotiate: Special service used to select at run time the EAP service to be used to authenticate the client.
  - CRL support
- HTTP digest authentication for Session Initiation Protocol (SIP) and web servers
- IETF RADIUS tunnel support (RFC 2867, RFC 2868)
- Automatic and customizable reply-message generation
- Chaining of authentication and authorization service through the environment attributes
- LDAP remote server's bind-based authentication

Accounting

- Local file
  - Store accounting records in a single file or multiple files
  - Automatic file rollover based on file age, size, or specific time
- Proxy
  - Option to ignore acknowledgements and continue processing
- Database
  - Write accounting records directly to an Oracle or MySQL database or LDAP directory
  - Schema independent
  - Buffering option for higher throughput and fault tolerance
- Chaining of accounting service through the environment attributes

Proxy, Database, and LDAP Configuration

- Define a list of remote systems to be used in failover or round-robin modes
- Accept All, Reject All, and Drop Packet outage policies available when no remote systems are available
- Define the individual characteristics of each remote system, for example, ports, timeouts, retries, or reactivate timers
- Sophisticated algorithms to detect status of remote systems

Request Processing Decisions Based on Rules and Policy Engine

- Process requests using different methods; for example, use LDAP for some access requests, the internal database for others
- Process requests using a combination of these methods; 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
- Split authentication and authorization by selecting one method for authentication and another for authorization (One-Time Password [OTP] server and Oracle database, for example)
- Decide which method to use based on attributes in the request or on Cisco Access Registrar's environment variables, such as source or destination IP address or User Datagram Protocol (UDP) port
- Decide which service needs to be chained based on attributes on the Cisco Access Registrar's environment variables, such as the reauthentication service, reauthorization service, and reaccounting service
- Easy method selection based on DNS domain, username prefix, dialed number, calling number, or NAS, using the Cisco Access Registrar policy engine

Resource Allocation and Session Management

- Built-in feature to track user sessions and allocate resources
- Options to store active session information to an external database like Oracle
- Enforcement of session limits per user and per group
- Allocation of addresses from IP pools
- Allocation of home agents and on-demand address pools
- Real-time query of the session table using the command-line interface (CLI), XML over UDP, or RADIUS
- Ability to add custom information to the session table
- Ability to configure which attributes to store in the session table
- Manual release of sessions and resources
- Query and release sessions based on session age, username, NAS, and other criteria
- Release sessions and generate Packet of Disconnect (PoD)
- Automatic session release when accounting stop is lost (inactivity timeout)
- Automatic session release when accounting on/off is detected (system accounting)
- In an environment with multiple Cisco Access Registrars, ability to designate one Cisco Access Registrar to manage all sessions to avoid bypass of session limits and to allocate IP addresses and other resources centrally
- Session information not lost even if Cisco Access Registrar or the system is restarted
- Session tracking for accounting-only servers
- Configurable session key based on any attributes present in the incoming request
- Ability to send Change of Authorization (CoA) request

- Ability to count the number of user sessions
- Ability to query cached attributes through the query session

System Tuning and System Configuration

- Configure Cisco Access Registrar to listen on multiple UDP ports
- Specify which network interfaces to use
- Set the number of simultaneous requests to be processed
- Regular and advanced duplicate detection features
- Extensible attribute dictionary
  - 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
- Specify log file rollover rules

Troubleshooting and Monitoring

- Multilevel debugging output
- Real-time query of processing counters
- Reset processing counters without restarting Cisco Access Registrar
- Query status of all Cisco Access Registrar processes and utilities
- Log files for each Cisco Access Registrar process
- Audit log of all configuration changes
- Direct logs to a syslog server
- RADIUS Simple Network Management Protocol (SNMP) RFC 2618-21 support
- SNMP traps generated for critical events
- Utility to generate RADIUS requests

Configuration

- Powerful command-line configuration utility with interactive/noninteractive full and view-only modes
- Noninteractive modes allow for configuration automation and operations support system (OSS) integration
- 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 Access Registrar
- Specify multiple RADIUS clients with a single definition

Resilience

- Automatic configuration replication to other Cisco Access Registrar servers (server redundancy)
- Specify lists of alternate remote systems for each processing method (remote-system redundancy)
- Specify multiple methods to process a request (processing-method redundancy)
- Automatic server restart

Customization

- Add custom logic to the request processing flow using Tcl, C or C++, or Java
  - Access request and response packets
  - Modify processing decisions in real time
  - Target specific requests with multiple callout points
- Create custom processing methods

Solutions

- Cisco PDSN for CDMA2000 mobile wireless
  - Home agent allocation for balanced home agent access
  - Null password support
  - Multiple accounting start/stop detection for roaming users
  - CDMA2000 vendor-specific attribute support
  - Prepaid billing
  - Quality of service (QoS) and remote address accounting attributes support
  - PoD during packet data serving node (PDSN) handoff
  - Mobile Node-Home Agent (MN-HA) shared key distribution for mobile IP
  - Domain Name System (DNS) update for IP reach ability
  - Change of Authorization (CoA)
- Public wireless LAN solution for service providers
- Cisco IOS® Software On-Demand Address Pool Manager
- Dynamic, variable-size address pool assignment for Multiprotocol Label Switching (MPLS) VPNs
- Broadband aggregation
- Trusted-ID authorization for transparent autologon
- WiMAX support based on NWG stage 3 document
- Other solutions
  - Cisco Gateway GPRS Support Node (GGSN) for GPRS mobile wireless
  - Cisco Any Service, Any Port (ASAP) solutions

System Requirements

Tables 1 and 2 list system requirements for Cisco Access Registrar 5.0.

Table 1. Server System Requirements: Large Service Provider Network

Demo Server Requirements		
Operating system	Solaris 10	Linux RHEL 5.3
Model	SPARC Enterprise T5220	X86
CPU type	UltraSPARC-T2 (SPARC V9)	Intel Xeon CPU 3.40 GHz
CPU number	8 cores (8 threads each)	4
CPU speed	1165 MHz	3.40 GHz
Memory (RAM)	8 GB	8 GB
Swap space	10 GB	10 GB
Disk space	2 x 72 GB	1 x 146 GB

Table 2. Server System Requirements: Small Service Provider Network

Demo Server Requirements		
Operating system	Solaris 10	Linux RHEL 5.3
Model	SPARC Enterprise T5220	X86
CPU type	UltraSPARC-T2 (SPARC V9)	Intel Xeon CPU 3.40 GHz
CPU number	4 cores (8 threads each)	4
CPU speed	1165 MHz	3.40 GHz
Memory (RAM)	4 GB	4 GB
Swap space	4 GB	4 GB
Disk space	20 GB	20 GB

Note: Service providers with subscriber bases of more than 300,000 fall under the larger service provider network.

Download the Software

To download Cisco Access Registrar Software, visit the Cisco Software Center.

Service and Support

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 Access Registrar, visit http://www.cisco.com/go/car/, 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.**

Printed in USA C78-566189-01 01/11