Cisco Access Registrar 5.1

General Information

Q. What is Cisco® Access Registrar?

A. Cisco Access Registrar is a RADIUS and Diameter server that is designed to meet the specific authentication, authorization, and accounting (AAA) needs of service providers, including deployment, performance, scalability, resilience, and extensibility requirements.

Q. What are the major enhancements for Cisco Access Registrar 5.1?

A. New features in Cisco Access Registrar 5.1 include:

- Extension of WLAN authentication mechanisms to the Home Subscriber Server (HSS): Cisco Access Registrar now supports Subscriber Identity Module (SIM) and Universal SIM (USIM) authentication for data access against the newer generation subscriber database, HSS, through a Diameter interface.
- Extended Oracle support: Includes native Oracle database interface support.
- Support for the Solaris ZFS file system: Provides data integrity, support for high storage capacities, and more.
- Support for stored procedures on an Oracle server.
- Platform support: Solaris 10, RedHat Enterprise Linux (RHEL) 5.3/5.4/5.5, femtocell support, and virtualization support; Oracle VM Server for SPARC (previously called Logical Domains, LDoms) and VMware ESXi 4.1.

Q. What are the benefits of Cisco Access Registrar 5.1?

A. Cisco Access Registrar delivers a full-featured, customizable RADIUS and Diameter server that focuses service providers on delivering revenue-generating services. With one common platform, the solution simultaneously supports both RADIUS and Diameter protocols, allowing operators to protect investments in legacy applications and services and deploy new services supported by Diameter. The solution is fast and scalable to support large service deployments and supports multiple access technologies, multiple subscriber data stores, and broad integration with external systems.

Q. How widely is Cisco Access Registrar deployed?

A. Cisco Access Registrar is a mature, carrier-class RADIUS and Diameter server that has been deployed worldwide by more than 200 service providers, both large and small, since 1998.

Q. What are the basic components in Cisco Access Registrar and how are they implemented?

A. Cisco Access Registrar basically consists of UNIX daemons and a very fast internal database. The internal database stores the AAA configuration and can also be used for storing user profiles. Cisco Access Registrar consists of three main functional units:

- **Policy Engine:** A robust and extensible method of imposing per packet policies
- **AAA server:** A RADIUS server designed from the ground up for performance, scalability, and extensibility for deployment in complex service provider environments

- **Session Manager:** Keeps track of active user sessions and allows real-time query from external applications; allocates resources such as IP address per user, per group session limiting, and others

Q. Is Cisco Access Registrar scalable?

A. Directory and database capabilities allow Cisco Access Registrar to support authentication and authorization for millions of users. Multiple Cisco Access Registrar servers can reference a distributed directory or database, and Cisco Access Registrar supports replication of its internal database to allow multiple servers to be similarly configured. In addition, the multithreaded architecture provides performance that scales with additional CPUs. Finally, an external session manager allows tens of millions of simultaneous active sessions. Together these features allow Cisco Access Registrar to scale to support large service deployments with high call rates.

Q. What is Cisco Access Registrar Director?

A. Cisco Access Registrar Director provides:

- Intelligent load balancing
- Accounting support
- Proxy and extension point scripting (EPS) functionality
- Ability to redirect the packets based on rule and policy engine or customization with extension point scripting
- IPv4 and IPv6 interface support
- Exposure of a single IP address from the network access server (NAS) for performance up to 16,000 transactions per second (TPS)

No other service (including authentication service, resource management, and session management) is available as part of the Cisco Access Registrar Director license.

Q. Is it possible to use Cisco Access Registrar Director as a RADIUS/Diameter load balancer?

A. Cisco Access Registrar Director can be used when RADIUS or Diameter packets need to be manipulated (for example, when attributes are added, modified, or deleted on the fly) and it is mainly used when it is necessary to proxy or load balance the packet based on a certain condition or a rule. Cisco Access Registrar Director has the intelligence to manipulate the packets using extension point scripts (C/C++/Java/Tool Command Language [Tcl]) and redirect the packets based on certain conditions.

Q. Does Cisco Access Registrar Director support multikey binding while being used as a Diameter load balancer?

A. Yes, Cisco Access Registrar Director supports binding based on any one attribute value pair (AVP) or combination of multiple AVPs.

Q. What session management features does Cisco Access Registrar have?

A. Cisco Access Registrar is capable of tracking active user sessions. By tracking these sessions, Cisco Access Registrar can enforce session limits on a per user or group basis. It also can manage shared resources including IP addresses and home-agent assignment. Session management can be configured on the same (local) server or an external server. Using local server session management, one can manage upto four million sessions per server while the external session manager can help scale upto tens of millions of sessions per server. Querying of session information through the command-line interface (CLI), XML, or RADIUS is possible. This can be used by external business applications to understand information about users/groups logged in and the resources consumed by them.

Q. What types of accounting and billing systems does Cisco Access Registrar support?

A. Cisco Access Registrar supports local flat-file accounting records, proxy RADIUS accounting, or writing records directly to an Oracle or MySQL database or a Lightweight Directory Access Protocol (LDAP) directory. In addition, Cisco Access Registrar can be configured to use a combination of these accounting methods when processing an accounting request. These methods also allow either offline transfers or direct feeds of accounting records into a billing server.

Q. Does Cisco Access Registrar come with an LDAP directory server?

A. No, Cisco Access Registrar does not provide an LDAP directory server. Cisco Access Registrar has been tested successfully with the Sun ONE Directory Server and Novell eDirectory. OpenLDAP provides an open source LDAP directory.

Q. Does Cisco Access Registrar support postpaid and prepaid subscriptions?

A. Cisco Access Registrar supports both prepaid and postpaid subscriptions and supports offline accounting.

To support postpaid subscriptions, Cisco Access Registrar can:

- Proxy RADIUS accounting messages to capable billing systems directly
- Write to a local file or a relational database management system(RDBMS), and billing systems can read from these
- Performa combination of these

To support prepaid subscriptions, Cisco Access Registrar can be integrated with billing systems using a set of predefined APIs. Cisco Access Registrar supports Cisco real-time billing and the IS835c prepaid standards.

Q. Which Extensible Authentication Protocol (EAP) authentication methods does Cisco Access Registrar support?

A. EAP methods supported by Cisco Access Registrar are:

- EAP-SIM
- EAP-AKA
- EAP-TLS
- EAP-TTLS
- EAP-MSChapV2
- EAP-MD5
- EAP-LEAP
- EAP-GTC
- Protected EAP
- EAP-Negotiate: Used to select a list of candidate EAP services that represent the allowable authentication methods in preference order

Q. How is centralized administration achieved in Cisco Access Registrar?

A. The Cisco Access Registrar replication feature can maintain identical configurations on multiple machines simultaneously. When replication is properly configured, changes an administrator makes on the primary or master server are propagated by Cisco Access Registrar to a secondary or member server. Replication eliminates the need to have administrators with multiple Cisco Access Registrar installations make the same configuration changes at each of their installations. Instead, only the master's configuration needs be changed,

and the member is automatically configured, eliminating the need to make repetitive, error-prone configuration changes for each individual installation. In addition to enhancing server configuration management, using replication eliminates the need for a hot-standby machine.

Q. What information does the Cisco Access Registrar server log?

A. The Cisco Access Registrar server maintains a comprehensive list of log files to record server statistics and user information. All the logs are stored locally in the UNIX file system as text files and allow easy deployment of tools that parse the log files. The files can be exported through file transfer. Cisco Access Registrar maintains the following logs:

- **Server log:** Logs server statistics such as reloads
- **Command log:** Logs administrator commands through the CLI and GUI
- **RADIUS log:** Logs RADIUS traffic information on the server, including successful and unsuccessful authentications with the reason for rejection, and so on
- **TPS log:** One file per day to hold the TPS information of the Cisco Access Registrar server for the day, once enabled
- **RADIUS traces:** The verbosity of this log can be set from the CLI and GUI. At maximum verbosity, it logs packet traces of each request and response, the internal services that processed the packet, and the extension point scripts, if any, that were applied on the flow

Q. What are the types of deployment available for Cisco Access Registrar?

A. Cisco Access Registrar can be deployed with session management and without session management. In each setup both active-active and active-standby deployments are available.

Q. Is this offering supported by the Cisco Technical Assistance Center (TAC)?

A. Yes, the Cisco TAC, worldwide, has received Cisco Access Registrar training and provides 24-hour support.

Technical Information

Q. How does Cisco Access Registrar support subscriber provisioning for AAA services?

A. Subscribers can be provisioned through a CLI and a GUI. The CLI supports both interactive and noninteractive modes. The noninteractive mode allows batch processing of commands and can be used to integrate with other provisioning systems. The subscriber data is usually stored on an existing external database including Oracle, MySQL, Microsoft Active Directory (AD), and LDAP with which Cisco Access Registrar can be integrated. The CLI/GUI is typically used to configure specific configurations such as the various services, policies, scripts, and more.

Q. What, if any, additional software is needed to use Cisco Access Registrar?

A. Apart from a fully patched and supported version of the operating system, Cisco Access Registrar is self-contained. A fast, built-in database stores the server configuration and user information. No extra software is required to enforce user or group session limits, allocate IP addresses from IP pools defined in Cisco Access Registrar, configure Cisco Access Registrar to act as a RADIUS proxy, or to use the configuration replication feature.

Note: A graphical user interface is available for Cisco Access Registrar. To enable the GUI, the server should have Java Runtime Environment (JRE) 1.5.x installed.

Q. Is Cisco Access Registrar compatible with equipment from other vendors?

A. Yes. Cisco maintains compatibility with the latest RADIUS and Diameter standards to help ensure that Cisco Access Registrar is interoperable with any RADIUS and Diameter-compliant client, regardless of vendor. In addition, Cisco Access Registrar has an attribute dictionary that comes predefined with the attributes of other third-party vendors, and this dictionary is completely customizable such that attributes can be added, edited, or deleted at any time.

Q. What protocols, ports, or secure transmission methods are used between the client and the Cisco Access Registrar server?

A. For administration, TCP ports 2785 and 2786 are used. These ports are not configurable. The administrator password is never sent across the wire in clear text. The Simple Network Management Protocol (SNMP) daemon provided with Cisco Access Registrar uses standard SNMP ports. For RADIUS request processing, the network interfaces and ports used are configurable. By default, Cisco Access Registrar listens on ports 1645 and 1646 on all interfaces.

Q. What external data stores does Cisco Access Registrar support?

A. Cisco Access Registrar can be integrated with a variety of 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).

Q. What platforms are supported by Cisco Access Registrar?

A. Supported operating systems include RHEL 5.3, 5.4, and 5.5 and Solaris 10 and supported file systems include UFS and ZFS for Solaris. Cisco Access Registrar also can run in a virtualized environment Oracle VM Server for SPARC (previously called Logical Domains, LDoms) and VMware ESXi 4.1.

Q. What is ZFS?

A. In computing, ZFS is a combined file system and logical volume manager. The features of ZFS include data integrity (for example, protection against bit rot), support for high storage capacities, snapshots and copy-on-write clones, continuous integrity checking and automatic repair, RAID-Z and native NFSv4 access control lists (ACLs). ZFS is implemented as open-source software and licensed under the Common Development and Distribution License (CDDL).

Q. Can Cisco Access Registrar process RADIUS/Diameter requests differently based on attributes in the request?

A. Yes. Cisco Access Registrar can be configured to dynamically decide how to process requests based on any attribute in the packet, including, but not limited to, username prefix or suffix, dialed number, or calling number. An access request can be processed using information in an LDAP directory server or an Oracle or MySQL database, for example, forwarded to another RADIUS/Diameter server, or handled through a combination of these methods. An accounting request can be processed locally into a file, forwarded to another RADIUS/Diameter server, written to a database, or processed using a combination of these methods.

Q. Can Cisco Access Registrar be configured to modify attributes in a RADIUS or Diameter packet?

A. In addition to the authorization process, in which attributes stored in Cisco Access Registrar's internal database or external database are returned in an access-accept packet, Cisco Access Registrar allows attributes in a RADIUS/Diameter request, response, or proxy packet to be added, modified, or deleted. Cisco Access Registrar architecture incorporates the highest level of extensibility and exposes multiple points in the process flow within the server where custom logic can be applied. These points are referred to as extension points. Cisco Access Registrar supports extension point scripting in Tcl, C/C++, or Java. EPS allows service

providers to examine, change, or delete attributes in the request. This can be used to develop and deploy custom logic for user authentication, authorization, and accounting. For example, service providers can identify and modify username suffixes or prefixes as necessary and proxy the request to another designated AAA server for further processing. Any attributes can be analyzed for illegal characters and reformatted. In addition to being able to access attributes in the request and response, service providers can use EPS to communicate with Cisco Access Registrar at predefined points during packet processing by accessing the Cisco Access Registrar environment variables.

Q. What ports are available in Cisco Access Registrar?

A. The following ports are available:

- Default authentication/authorization and accounting port for Linux -1812 and 1813; and for Solaris -1645 and 1646
- Radius remote server - 1645/1812
- LDAP - 389
- Oracle - 1512
- MAP gateway - Any port
- Prepaid - Any port
- Domain authentication - 2004/2005
- Dynamic DNS - 53
- SNMP - 161
- HTTP (GUI) - 8080
- HTTPS - 8443

Accounting Messages

Q. What accounting messages are supported in Cisco Access Registrar?

A. Cisco Access Registrar supports RADIUS accounting, and supported accounting-status-type messages include Acct-Start/Stop/Interim-update/ON/OFF. A complete list of supported accounting attributes is available at http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.1/user/guide/a_attrib.html.

Cisco Access Registrar also supports writing accounting records to a local flat file, proxy to another RADIUS server, or to an external Oracle or MySQL database or LDAP directory. In addition, Cisco Access Registrar can be configured to use a combination of these accounting methods when processing an accounting request.

For more information, please visit http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.1/user/guide/accountg.html.

Q. How does Cisco Access Registrar communicate using Oracle Call Interface library files?

A. Cisco Access Registrar 5.1 introduced a new Oracle thin driver "OCILIB" which replaces the unix ODBC and Easysoft Oracle drivers for a direct interface mechanism to Oracle client libraries through the Oracle Call Interface API. This facilitates interaction with the latest and upcoming versions of Oracle database servers.

Authentication/Authorization/Accounting

Q. How can Cisco Access Registrar integrate with existing investments into subscriber management technology?

A. Cisco Access Registrar can be integrated with external databases such as Oracle, MySQL, LDAP, Active Directory, Home Location Register (HLR) and HSS using interfaces like ODBC, LDAP, JDBC, and Diameter.

Q. Is it possible to define a default user during the authentication process if the specific user in the request message is not in the userlist? Or, if an indication is received indicating that the user match failed, is it possible to reauthenticate to a different user/userlist?

A. If username match failed during the initial authentication phase, it is possible to reauthenticate (reauthorize, reaccount) the same user request using the Dynamic Service Authorization (DSA) feature.

You can find more information on DSA at http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.0/user/guide/features.html#wp1017196.

Q. Is Cisco Access Registrar able to reject an authentication request on the basis of RADIUS/Diameter attributes other than the user credentials?

A. Cisco Access Registrar supports the concept of check items. Check items are lists of RADIUS/Diameter AVPs that are associated with user groups or individual users Cisco Access Registrar architecture incorporates the highest level of extensibility and supports custom Tcl, C/C++, or Java scripts that can be deployed at numerous API points that Access Registrar exposes. This can be used to develop and deploy custom logic for user authentication or authorization.

Q. Is media access control (MAC) authorization supported in Cisco Access Registrar? If so, how is this done?

A. For MAC authentication Cisco Access Registrar can verify that the MAC in the incoming access request is the one that is allowed for a user by looking up the subscriber's profile. This can be achieved using the "check item mappings" option, which is available for subscribers provisioned in the local database as well as for those provisioned in an external LDAP/Oracle server. The solution also is able to insert custom logic using extension point scripts such as range comparisons and so on.

References:

- http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.1/user/guide/cfglocal.html#wp1041477
- http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.1/user/guide/odbc.html#wp1057614
- http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.1/user/guide/ldap.html#wp1041595

Extension Point Scripting

Q. What is extension point scripting in Cisco Access Registrar?

A. Cisco Access Registrar architecture incorporates the highest level of extensibility and exposes multiple points in the process flow within the server where custom logic can be applied. These points are referred to as extension points. Cisco Access Registrar supports EPS in Tcl, C/C++, or Java. EPS allows service providers to examine, change, or delete attributes in the request. This can be used to develop and deploy custom logic for user authentication, authorization, and accounting. As an example, service providers can identify and modify username suffixes or prefixes as necessary and proxy the request to another designated AAA server for further processing. Any attributes can be analyzed for illegal characters and reformatted. In addition to being able to access attributes in the request and response, service providers can use EPS to communicate with Cisco Access Registrar at predefined points during packet processing by accessing the Cisco Access Registrar environment variables.

Q. What are the differences in performance and stability between C/C++ and Java-based extensions? It appears that the Java implementation is relatively new. Has it been stressed? Is one recommended over the other?

A. Many Cisco partners and large customers are extensively using Java-based extensions. From a performance perspective C/C++ maybe faster that an equivalent Java code, but they are equally stable.

Q. What are the various logging mechanisms available in Cisco Access Registrar?

A. Cisco Access Registrar uses three levels of logging - Error, Warning, and Info - while printing messages in logs.

For extensive debugging, there also exists an option called “trace.” The trace level governs how much information is displayed about the contents of the packet. When the trace level is zero, no tracing is performed. The higher the trace level, the more information is displayed. The highest trace level currently used by the server is trace level five.

More information on how to enable “trace” is available at http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/5.0/user/guide/aregcmd.html#wp1041828.

Network Management Support

Q. What network management support methods does Cisco Access Registrar provide?

A. Cisco Access Registrar provides SNMP MIBand trap support for users of network management systems. The supported MIBs enable the network management station to collect state and statistic information from a Cisco Access Registrar server. The traps enable Cisco Access Registrar to notify interested network management stations of failure or impending failure conditions. SNMP traps enable a standard SNMP management station to receive trap messages from a Cisco Access Registrar server. These messages contain information indicating whether a server was brought up or down, or whether a proxied remote server is down or has come back online.

Q. What SNMP network management system support is included with Cisco Access Registrar?

A. The SNMP network management architecture consists of managed devices, SNMP agents, and network management stations (NMSs). An NMS is an administration workstation that polls management agents for information and provides control information for agents. A network management system can also accept trap messages when an asynchronous event occurs on a managed device. An SNMP agent or daemon is a software module running on a managed device that is responsible for recording performance statistics and events in a database called a management information base (MIB) and for communicating with the NMS. When an NMS requests information, the SNMP agent processes the request, acquires information from the management database, and forwards the information to the NMS. The SNMP agent can also accept control information from the NMS.

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 C67-688557-01 12/12