Cisco Prime Access Registrar

General Information

Q. What is Cisco Prime™ Access Registrar?

A. Cisco Prime Access Registrar is a 3GPP-compliant 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 benefits of Cisco Prime Access Registrar?

A. Cisco Prime 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. What are the major enhancements for Cisco Prime Access Registrar 6.1?

A. New features in Cisco Prime Access Registrar 6.1 include:

- Support for 3GPP compliance

- Translation of incoming RADIUS requests and responses to Diameter and vice versa

- Simplified GUI/command-line interface (CLI) mechanism to easily choose the correct authentication, authorization, and accounting services required for processing a packet

- Support for EAP-AKA-Prime (EAP-AKA') protocol

- Quintets to triplets translation that allows EAP-SIM authentication from an EAP-AKA/EAP-AKA' source

- Session management and query support for Diameter sessions

- Group services support for Diameter

- Tool Command Language (Tcl) and Java scripting for Diameter

- IPv6 support for external database servers, including Lightweight Directory Access Protocol (LDAP), Oracle, and MySQL, and access over HTTP and Simple Network Management Protocol (SNMP)

Q. What are the major enhancements for Cisco Prime Access Registrar 6.0?

A. New features in Cisco Prime Access Registrar 6.0 include:

- Support for seamless Wi-Fi data offload through the ability to interface directly with the Home Location Register (HLR) through an M3UA/SIGTRAN interconnectivity layer using EAP-SIM/EAP-AKA supported on Linux operating systems variant

- Smart grid identity and access management on IPv6 networks. This is achieved using the Elliptic Curve Cryptographic (ECC)-based certificate validation and also supports TACACS+ authentication and command authorization and accounting

- Extension of Red Hat Enterprise Linux (RHEL) support to include 6.0, 6.1, and 6.2

- Extension of platform virtualization support to include VMware 5.0

- Extension of clustering for high availability to include RHEL
- New networkwide licensing that allows an operator to purchase licensing to meet the sum of all individual server requirements and obtain better pricing. It is no longer a requirement to purchase a base license per server (a base license is now required per region); rather, operators can introduce additional servers as needed per network requirements - as long as they are within the overall licensed limits
- New licensing options with options for licensing based on either transactions per second (TPS) or Concurrent Online/Active Subscriber/Device Session (SUB). Licenses are available in various slabs of granularity to match specific requirements of the network. Existing customers that utilize the TPS licensing model will be allowed to migrate to the SUB model.

Q. How widely is Cisco Prime Access Registrar deployed?

A. Cisco Prime 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 Prime Access Registrar and how are they implemented?

A. Cisco Prime 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 Prime 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 limits, and others

Q. Is Cisco Prime Access Registrar scalable?

A. Directory and database capabilities allow Cisco Prime Access Registrar to support authentication and authorization for millions of users. Multiple Cisco Prime Access Registrar servers can reference a distributed directory or database, and Cisco Prime 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 Prime Access Registrar to scale to support large service deployments with high call rates.

Q. What is Cisco Prime Access Registrar Director?

A. Cisco Prime 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 TPS

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

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

A. Cisco Prime Access Registrar Director can be used when RADIUS 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 Prime Access Registrar Director has the intelligence to manipulate the packets using extension point scripts (C/C++/Java/Tcl) and redirect the packets based on certain conditions.

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

A. Cisco Prime Access Registrar is capable of tracking active user sessions. By tracking these sessions, Cisco Prime 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 up to four million sessions per server while the external session manager can help scale up to tens of millions of sessions per server. Querying of session information through the 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 Prime Access Registrar support?

A. Cisco Prime 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 Prime 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 Prime Access Registrar come with an LDAP directory server?

A. No, Cisco Prime Access Registrar does not provide an LDAP directory server. Cisco Prime 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 Prime Access Registrar support postpaid and prepaid subscriptions?

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

To support postpaid subscriptions, Cisco Prime 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
- Perform a combination of these

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

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

A. EAP methods supported by Cisco Prime Access Registrar are:

- EAP-SIM/AKA/AKA' over M3UA/SIGTRAN or SWx (over Diameter)
- 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 Prime Access Registrar?

A. The Cisco Prime 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 Prime Access Registrar to a secondary or member server. Replication eliminates the need to have administrators with multiple Cisco Prime 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 Prime Access Registrar server log?

A. The Cisco Prime 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 Prime 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 Prime 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 Prime Access Registrar?

A. Cisco Prime 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 Prime Access Registrar training and provides 24-hour support.

Technical Information

Q. How does Cisco Prime 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 Prime 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 Prime Access Registrar?

A. Apart from a fully patched and supported version of the operating system, Cisco Prime 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 Prime Access Registrar, configure Cisco Prime Access Registrar to act as a RADIUS proxy, or to use the configuration replication feature.

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

Q. Is Cisco Prime 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 Prime Access Registrar is interoperable with any RADIUS and Diameter-compliant client, regardless of vendor. In addition, Cisco Prime 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 Prime 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 Prime Access Registrar uses standard SNMP ports. For RADIUS request processing, the network interfaces and ports used are configurable. By default, Cisco Prime Access Registrar listens on ports 1645 and 1646 on all interfaces.

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

A. Cisco Prime 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 Prime Access Registrar?

A. Supported operating systems include RHEL 5.3, 5.4, 5.5, 6.0, 6.1, and 6.2 and Solaris 10[*] and supported file systems include UFS and ZFS for Solaris. Cisco Prime Access Registrar also can run in a virtualized environment Oracle VM Server for SPARC (previously called Logical Domains, LDoms) and VMware ESXi 5.0.

[*] 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.

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 Prime Access Registrar process RADIUS/Diameter requests differently based on attributes in the request?

A. Yes. Cisco Prime 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 Prime 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 Prime Access Registrar's internal database or external database are returned in an access-accept packet, Cisco Prime Access Registrar allows attributes in a RADIUS/Diameter request, response, or proxy packet to be added, modified, or deleted. Cisco Prime 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 Prime 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 Prime Access Registrar at predefined points during packet processing by accessing the Cisco Prime Access Registrar environment variables.

Q. What ports are available in Cisco Prime 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 Prime Access Registrar?

A. Cisco Prime 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 in the User Guide.

Cisco Prime 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 Prime Access Registrar can be configured to use a combination of these accounting methods when processing an accounting request.

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

A. An Oracle thin driver "OCILIB" provides 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 Prime Access Registrar integrate with existing investments into subscriber management technology?

A. Cisco Prime Access Registrar can be integrated with external databases such as Oracle, MySQL, LDAP, and Active Directory, using interfaces like ODBC, OCI, LDAP, JDBC, and subscriber repositories like HLR/HSS using M3UA/SIGTRAN 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 in the User Guide.

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

A. Cisco Prime 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 Prime 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 Cisco Prime 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 Prime Access Registrar? If so, how is this done?

A. For MAC authentication Cisco Prime 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.

Extension Point Scripting

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

A. Cisco Prime 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 Prime 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 Prime Access Registrar at predefined points during packet processing by accessing the Cisco Prime 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++ may be faster than an equivalent Java code, but they are equally stable.

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

A. Cisco Prime 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.

Network Management Support

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

A. Cisco Prime Access Registrar provides SNMP management information base (MIB) and trap support for users of network management systems. The supported MIBs help enable the network management station to collect state and statistic information from a Cisco Prime Access Registrar server. The traps help enable Cisco Prime Access Registrar to notify interested network management stations of failure or impending failure conditions. SNMP traps help enable a standard SNMP management station to receive trap messages from a Cisco Prime 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 Prime 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 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.

Printed in USA

C67-730452-00   12/13