Cisco Access Registrar 5.0

General Questions

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 is new for Cisco Access Registrar 5.0?

A. Cisco Access Registrar 5.0 is a major release with new features including the IP Multimedia Subsystem (IMS)–ready platform and enhancements and bug fixes that will benefit a number of current and potential customers. The primary features of Cisco Access Registrar Release 5.0 include Diameter protocol support, IPv6 support, Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA), a new GUI with enhanced configration interface, session scalability (writing the session information to an exernal Oracle server), and WiMAX lawful intercept and WiMAX compliance enhanced to support the latest Network Working Group (NWG) stage 3 document version 1.3.1. Other enhancements include Lightweight Directory Access Protocol (LDAP) accounting write, dynamic SQL, and stored procedures. Customers can also install Access Registrar in a virtualization environment using VMware ESX. Support for Red Hat Enterprise Linux 5.3, Sun clustering in logical domains (LDOMs), and Veritas clustering is provided for achieving high availability. Finally, Access Registrar Director, which can be used as a load balancer or in an extensive proxy scenario, is introduced.

Q. What is Access Registrar Director?

A. 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 where 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.

Q. What are the advantages and limitations over the Application Control Engine (ACE) in a load balancing scenario?

A. Access Registrar Director can be used when the packets need to be manipulated, for example, when attributes are added, modified, or deleted on the fly, and it is mainly used where we have to proxy or load balance the RADIUS or Diameter packet based on a certain condition or a rule. Access Registrar 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 that normally ACE does not have. Access Registrar Director can handle up to 4000 transactions per second (TPS) when used in load balancing or in a proxy scenario. With the help of group service you can proxy the packets using logical operators AND/OR/Parallel AND & Parallel OR to multiple targets at the same time.

Q. How does Access Registrar Director maintain the sticky information while load balancing?

A. Cisco Advanced Services can be contacted to write a script to maintain the sticky information when Access Registrar is used in a load balancing mode.

Q. Do I need to buy an additional license for Access Registrar Director?

A. Access Registrar Director requires a separate license, and the customer needs to purchase it additionally.

Q. What are the benefits of Cisco Access Registrar?

A. Cisco Access Registrar delivers a full-featured, customizable RADIUS and Diameter server that focuses service providers on delivering revenue-generating services. The latest release, Cisco Access Registrar 5.0, provides functionality to deliver the latest AAA server technology for broadband and mobile wireless networks, wireless LANs, and public wireless LANs.

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 numerous large enterprises and service providers, both large and small, since 1998.

Technical Questions

Q. What hardware specification should I use?

A. Cisco Access Registrar supports Solaris in a Sun SPARC platform and Linux in an X86 platform. Which product to choose depends on the customer and the customer's AAA reqirements. For hardware specifications, please see the Cisco Access Registrar 5.0 Release Notes.

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. It has a fast, built-in database that 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's attribute dictionary comes predefined with the attributes of other third-party vendors, and this attribute dictionary is completely customizable so attributes can be added, edited, or deleted at any time.

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. Additionally, Cisco Access Registrar supports replication of its internal database to allow multiple servers to be similarly configured. Cisco Access Registrar's multithreaded architecture provides performance that scales with additional CPUs. Together, these features allow Cisco Access Registrar to scale to support large service deployments with high call rates.

Q. What protocols, ports, or secure transmission methods are used between the client and 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 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 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.

Basically Cisco Access Registrar consists of three 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 other methods.

Q. What standards are supported by Cisco Access Registrar?

A. Cisco Access Registrar supports the following RFCs:

- 2865 RADIUS
- 2866 RADIUS Accounting
- 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
- 2868 RADIUS Attributes for Tunnel Protocol Support
- 3576 Dynamic Authorization Extensions (updates RFC 2869, Packet of Disconnect [PoD] support only)
- 3579 RADIUS Support for Extensible Authentication Protocol (EAP) (updates RFC 2869)
- 2618 RADIUS Authentication Client MIB
- 2619 RADIUS Authentication Server MIB
- 2620 RADIUS Accounting Client MIB
- 2621 RADIUS Accounting Server MIB
- 4186 Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)

Cisco Access Registrar supports the following drafts/documents:

- Digest Authentication over RADIUS (draft-sterman-aaa-sip-00.txt)
- EAP-SIM draft 11 (draft-haverinen-pppext-eap-sim-11.txt)
- WiMAX support as per NWG version 1.3.1 of the stage III document (WiMAX Forum)

Q. Can Cisco Access Registrar process RADIUS 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, forwarded to another RADIUS 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 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.

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

A. Cisco Access Registrar supports the concept of check items. Check items are a list of RADIUS attribute value pairs that are associated with user groups or individual user profiles. On successful completion of legacy authentication, Access Registrar verifies the attributes in the check item list with those in the requests, and the values should match for successful response.

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. What are Cisco Access Registrar extensions?

A. Cisco Access Registrar provides a number of extension points where customers or system integrators may extend the logic of the product through C/C++ shared libraries, Java, or Tcl scripts. These extension points allow access to incoming and outgoing RADIUS/Diameter packets for complete processing control. Extension points also support the integration of completely proprietary AAA services with a RADIUS/Diameter front end.

Q. What is the use of Cisco Access Registrar's Class attribute?

A. Cisco Access Registrar supports the Class attribute.

When the DetectOutOfOrderAccountingPacket property is enabled (set to TRUE), a new Class attribute is included in all outgoing accept packets. The value for this Class attribute will contain the session magic number. The client will echo this value in the accounting packets, and this will be used for comparison.

The session magic number is a unique number created for all sessions when the session is created or reused and the DetectOutOfOrderAccountingPacket property is set to TRUE. The DetectOutOfOrderAccountingPacket property is used to detect out-of-order accounting stop packets in roaming scenarios by comparing the session magic number value in the session with the session magic number value contained in the accounting packet.

The value of 0xffffffff is considered by the Cisco Access Registrar server to be a wild card magic number. If any accounting stop packet contains the value of 0xffffffff, it will pass the session magic validation even if the session's magic number is something else.

The format of the class attribute is as follows:

```
<4-byte Magic Prefix><4-byte server IP address><4-byte Magic value>
```

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

A. Cisco Access Registrar is able to track user sessions. By tracking these sessions, Cisco Access Registrar can enforce session limits on a per user or group basis. It can also manage shared resources, including IP addresses, home-agent assignment, and on-demand address pools (for Multiprotocol Label Switching [MPLS] VPNs).

Cisco Access Registrar maintains an in-memory table of active user sessions. It can be configured to store RADIUS attributes in the session table. Cisco Access Registrar allows applications on the network to query this session table using either RADIUS or Extensible Markup Language (XML) queries from the 4.1 release.

Apart from writing the user session in an in-memory table, Cisco Access Registrar 5.0 supports writing the session information to an external Oracle server, which will eventually break the session limit of 4 million in memory in Access Registrar 4.2.

Cisco Access Registrar can query sessions by their age and then release them and generate a PoD if necessary.

Session management can take place, independently, on each Cisco Access Registrar in the network, or one Cisco Access Registrar server can be designated to perform this function for the other Cisco Access Registrar servers in the network to provide centralized session management.

Q. How much memory does Cisco Access Registrar's session management require?

A. Each session can use up to a maximum of 8 kilobytes (KB). Normally it is much less than this.

Memory consumption will vary based on the number and types of resource managers used, by whether session notes are used, and by the number of sessions. Sessions are stored in one or more hash tables, so the size of the table grows linearly with the number of sessions. A customer reported that roughly 1 KB of memory per session was consumed for 4 million sessions. Session information is also stored on disk. A comparable amount of disk space is therefore also required during session management.

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 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 support Dynamic Host Configuration Protocol (DHCP) for IP address allocation?

A. No, Cisco Access Registrar does not support DHCP for IP address allocations.

Instead, it is possible to define IP pools within Cisco Access Registrar for allocation.

It may be possible to create a custom service in Cisco Access Registrar to do IP allocation through DHCP.

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 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.

Access Registrar supports offline accounting. For postpaid, Access Registrar is very loosely coupled with billing systems in the sense that:

- Access Registrar can proxy RADIUS accounting messages to billing systems directly
- Access Registrar writes into a local file or Open Database Connectivity (ODBC) database and the billing system can read from the database

Access Registrar supports online accounting. For prepaid, Access Registrar is tightly coupled with billing systems in the sense that:

- Access Registrar can be customized to talk to any external accounting agent. This is achieved by implementing a set of API functions defined by Access Registrar.

In case of postpaid or offline accounting, Access Registrar will only write the accounting records into an internal flat file or into an external database like Oracle or MySQL using the ODBC interface or into an external directory like LDAP using the LDAP interface. It is up to the agent to read the details from the databases.

Access Registrar supports Cisco real-time billing and the IS835c prepaid standards.

Q. Does Cisco Access Registrar support EAP authentication methods?

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-Negiotiate

Q. How is redundancy achieved in Cisco Access Registrar?

A. Cisco Access Registrar supports replication allowing configurations in a primary server to replicate multiple secondary servers <Given as per Cisco Access Registrar functionality>. This allows easy deployment of redundant architecture with the ease of maintaining a cluster of servers with identical configuration and centralized management.

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

A. 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 command-line interface (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
- **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. Does Cisco Access Registrar output any messages to help in troubleshooting?

A. Yes, Cisco Access Registrar has extensive logging. All the log files are in the logs directory of the Cisco Access Registrar installation. To get detailed troubleshooting output, turn on tracing by entering the following command in the aregcmd command-line interface utility:

```
trace /r 5
```

This will generate detailed server processing information to the logs/name RADIUS 1 trace file.

Q. How do I configure Cisco Access Registrar?

A. You use the command-line interface utility, aregcmd. It stores the configuration information in the internal database. From Access Registrar 5.0 release we have a new GUI for easy configration

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.

Q. What data imports and exports does this offering support? How is this achieved?

A. Cisco Access Registrar's configuration is stored in an embedded database. Cisco Access Registrar ships with backup and restore utilities (mcdshadow and keybuild, respectively) for this database.

To configure Cisco Access Registrar from another data source, Cisco Access Registrar commands have to be generated. These can be placed in a file and executed in one go. RADIUS accounting records are stored in flat text files for import into external databases.

Q. How does Cisco Access Registrar decide to mark a remote server as down or offline?

A. Cisco Access Registrar marks a remote server as down when it does not receive a response from it. It makes use of three properties in the RemoteServer object:

- MaxTries
- InitialTimeout
- ReactivateTimerInterval

Cisco Access Registrar waits InitialTimeout milliseconds (ms) for a response from the remote server. If it does not receive a response, it resends the request up to MaxTries times, doubling the previous timeout each time. If it has not received a response after MaxTries and it has not received responses from any other requests sent to the same remote server during the same period, it marks that server as down.

Checking whether it has received responses to other requests sent to the same remote server allows for the situation where the remote server is responding to some requests but not all and, therefore, is not down.

Cisco Access Registrar will wait ReactivateTimerInterval ms before marking the remote server as up again. Cisco Access Registrar will mark all remote servers as up after a reload.

Q. How do you use return attributes in Access-Accept?

A. For users stored in Cisco Access Registrar 3.0 and later, each user object has an Attributes subobject in which return attributes can be entered:

```
[ //localhost/Radius/UserLists/Default/bob ]
Name = bob
Description =
Password =
AllowNullPassword = FALSE
Enabled = TRUE
Group~ =
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
Attributes/
    Session-Timeout = 600
CheckItems/
```

The profile object may be used to define attributes to be used by many users. The profile object is defined once and then applied to each user that requires it.

For users stored in an LDAP directory or Oracle database, values may be stored in the user record and then mapped to the RADIUS attributes to be returned to the user. This mapping is done in the RemoteServer object.

Q. How do you add the new vendor-specific attributes (VSAs)?

A. Cisco Access Registrar has the extensibility to add new VSAs on the fly and they can be added under:

```
[ //localhost/Radius/Advanced/Attribute\ Dictionary/Vendor-Specific/Vendors/]
```

To add any VSA:

```
[ //localhost/Radius/Advanced/Attribute Dictionary/Vendor-Specific/Vendors]
Add Cisco
Cd Cisco
Name = Cisco
Description =
VendorID = 9
Type = SUB_ATTRIBUTES
VendorTypeSize = 8-bit
HasSubAttributeLengthField = TRUE
SubAttribute Dictionary/
Cd SubAttribute Dictionary
SubAttribute Dictionary/
Add Cisco-AVPair
Cisco-AVPair/
Name = Cisco-AVPair
Description =
SubAttribute = 1
Type = STRING
Min = 0
Max = 253
```

Customers can add their VSAs similar to the preceding one.

Q. How do you know which version of Cisco Access Registrar is running?

A. You can use pkginfo -l CSCOar or, in aregcmd, check the Version property in the RADIUS object:

```
--> ls /Radius
```

Q. What protocols, ports, or secure transmission are used between client and 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 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. How is the health number in aregcmd calculated in Cisco Access Registrar?

A. The number starts off at 10, indicating a “healthy” server.

The following things decrement the server's health:

- The rejection of an access request
- Configuration errors
- Running out of memory
- Errors reading from the network
- Dropping packets that cannot be read (because the server ran out of memory)

- Errors writing to the network

As you can see, if there are a few access rejects, it can bring down the server health. In production servers, the health value will usually be somewhere between 3 and 10 depending on the number of access rejects.

Q. Is there any way to get Cisco Access Registrar to log successful authentications?

A. Yes. By default, /Radius/Advanced/LogServerActivity is set to false.

This means that Cisco Access Registrar will only log rejected and dropped authentications to the name_radius_1_log log file. To log successful authentications as well, set its value to true.

License Questions

Q. What is the use of the Access Registrar Secondary license ?

A. When Access Registrar is deployed in two-tier architecture, Access Registrar server, which acts as a standby server (front end or back end) for an active Access Registrar server or as an active session management (back end) server, needs only the Access Registrar Secondary license.

Note: Access Registrar server with the Secondary license is not intended for regular traffic handling.

Q. Assuming an accounting message has been proxied to three additional servers from the Access Registrar server, how should it be counted—as one or three transactions?

A. Transactions are based on the number of AAA packets flowing into Cisco Access Registrar. In your accounting proxy scenario, the acct-start request should be counted as one transaction when proxied to multiple servers.

Each accounting request packet is counted as a single transaction and not as multiple transactions to each server to which it is proxied.

For example: Local/LDAP/ODBC/proxy service: PAP authentication = three transactions (1 Access-Request + 1 Accounting-Request (Start) + 1 Accounting-Request (Stop))

Q. Do we only count TPS between network access server (NAS) and Access Registrar or do we count all proxy peers as well? For instance, if we have 100 TPS between GGSN and Access Registrar and two proxy peers, do we count 100 or 100+100+100?

A. TPS count is based on the incoming traffic, that is, traffic between GGSN and Cisco Access Registrar, so it is 100.

Q. For the accounting interim, how do we take the interim updates properly into account?

A. As the number of interim updates is dependent on the actual number of session and the settings on the NAS, this has to be calculated on top:

```
E = C*D + (number of sessions * interim updates/ sec)
```

Q. What happens if the customer surpasses 100 percent of the TPS limit? Will some messages be discarded? Is there some buffer mechanism before messages are discarded?

A. Access Registrar has a buffer of 10 percent; beyond that there will be slight dip in the performance. For example, if the customer has a 100 TPS license, the Access Registrar server will handle up to 110 TPS, and beyond that also Access Registrar will not discard any packets but there will some performance impact.

If the incoming traffic is high beyond 110 percent of the total TPS license for a continuous 20 minutes, Access Registrar throws an error message. Note that Access Registrar does not drop any packets. Access Registrar licensing is purely honor based. It is recommended to purchase Access Registrar additional TPS licenses, which are available in ranges starting from 100, 200, 500, 1000, and 3000 TPS.

Information about Access Registrar license enforcement is available in the Access Registrar User Guide, under the section “Enforcement of TPS License.”

Q. What are notification log messages thrown by Access Registrar?

A. A warning message is logged every 5 minutes when the TPS count reaches an increased steady state in which the TPS count is in the range of 80 percent to 100 percent of the licensed TPS.

An error message is logged every 5 minutes when the TPS count reaches an increased steady state in which the TPS count is in the range of 100 percent to 110 percent of the licensed TPS.

Q. How does the notification message look in Access Registrar?

A. The error and warning messages are logged in the name_radius_1_log file.

Beyond 80 percent of the license utilization, Access Registrar will start sending warning messages.

Warning message: "Radius is currently using %d percent of the licensed %dTPS

Beyond 100 percent of the license utilization, Access Registrar will start sending error messages. Access Registrar doesn't drop the excess login, that is, beyond 110 percent of the license

Error log message: "Current license usage is %d percent of %dTPS which is %dTPS and exceeding licensed limits."

Q. What SNMP traps does Access Registrar send?

A. The carLicenseUsage trap is generated only after an increasing steady state is reached. Traps are generated only once in an increasing phase. The incoming traffic slabs defined for trap generation are 80 percent, 90 percent, 100 percent, and 110 percent of the licensed TPS.

If the TPS count drops below 80 percent of the licensed TPS for a steady state period of 20 minutes, Cisco Access Registrar marks it as a decreased steady state. Traps will be generated again only if Cisco Access Registrar observes a decreased steady state followed by an increased steady state of TPS falling under the slab (say 80 percent).

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

A. Cisco Access Registrar can be deployed with session management and without session management. In each setup we have both active-active and active-standby deployment.

With Session Management (clustering is required to handle the session management):

- **Active-active setup:** We need to have a load balancer in front to balance the AAA traffic between the two clusters. Each cluster will have an active Access Registrar server and a standby Access Registrar server. In this setup we need to have four Access Registrar servers, two per cluster in active-standby mode. So we need two Access Registrar Base licenses and the additional TPS license in the two active servers and two Access Registrar Secondary licenses for the two standby servers.
- **Active-standby setup:** Packets are directly sent to the primary/active Access Registrar server from the NAS (GGSN/PDSN/ASN GW). The redundancy is configured at the NAS level for high availability. Here again, we need to cluster the two servers in active-standby mode. Here we will have only two Access Registrar servers, both clustered inactive-standby setup. So we need one Access Registrar Base license and the additional TPS license in the active server and one Access Registrar Secondary license for the standby server.

Without Session Management (no clustering is required):

- **Active-active setup:** We need to have a load balancer in front to balance the AAA traffic between the two servers. No clustering is required as there is no session management. We need to have two Access Registrar Base licenses and the additional TPS license in each server as it is in active-active mode.

- **Active-standby setup:** Packets are directly sent to the primary/active Access Registrar server from the NAS (GGSN/PDSN/ASN GW). The redundancy is configured at the NAS level for high availability. Here again no clustering is required as there is no session management required. We need one Access Registrar Base license and the additional TPS license in the active server and one Access Registrar Secondary license for the standby server.

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 C67-566191-00 11/09