# AdvOSS AAA Server

**PRODUCT DATA SHEET**

Latest version of this Product Datasheet can be downloaded from
www.advoss.com/resources/datasheet/advoss-aaa-product-datasheet.pdf

# Table of Contents

# 1 AdvOSS AAA SERVER

AdvOSS RADIUS AAA Server is required by any communications service providers such as Telecoms, wired and wireless broadband providers in 3G, 4G, LTE or other technologies. It is needed to provide a real-time interface between service delivery functions and core functions like B/OSS, policy, rating, charging, service management and subscriber management.

AdvOSS AAA is a Carrier Grade high performance & scalable Server that provides Authentication, Authorization and Accounting over Radius Protocol.

It can be used by any telecom or other service provider to get a real-time AAA interface to backend billing and OSS system.

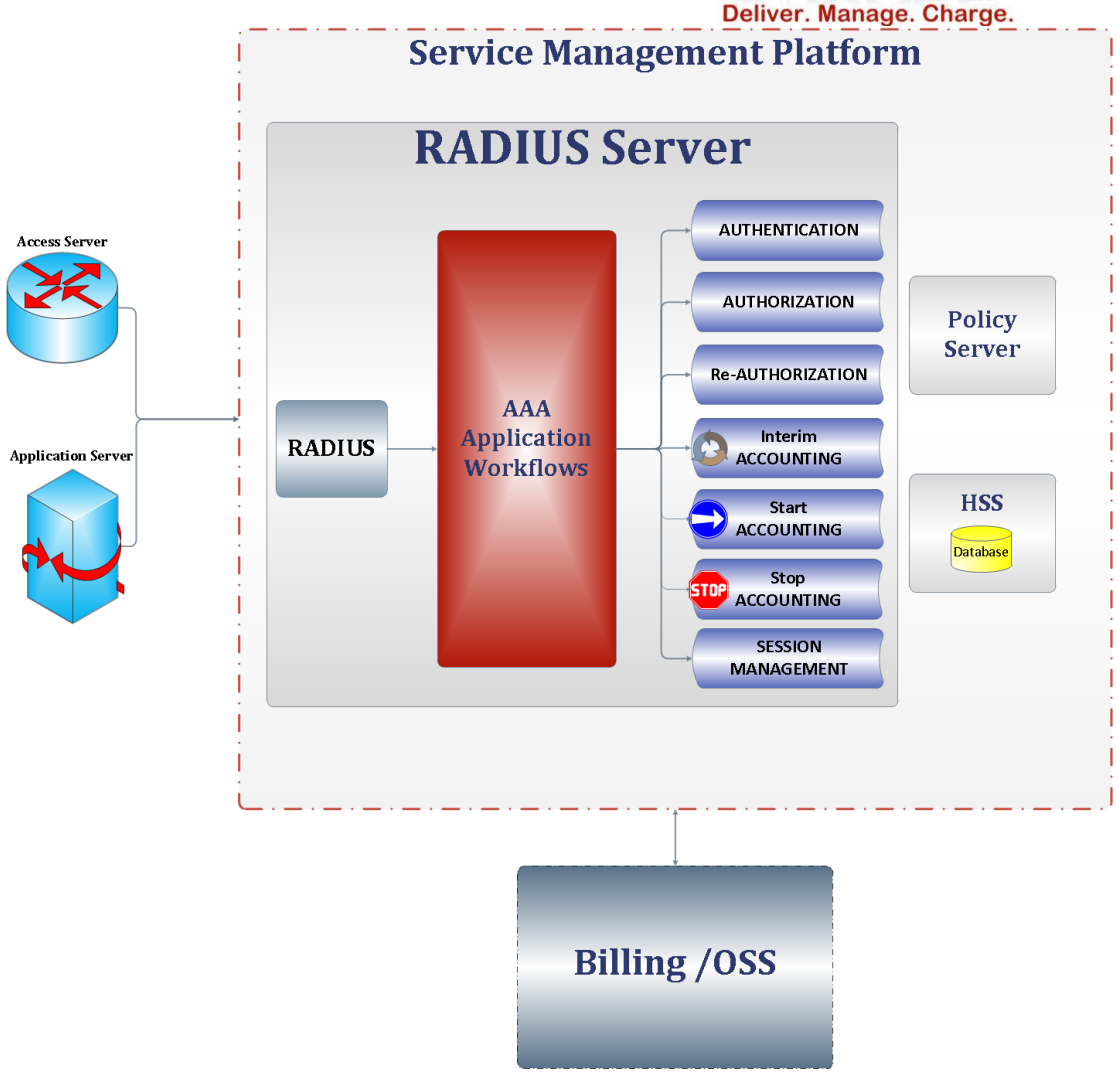
**Overview**

AdvOSS AAA provides customizable work-flows for Authentication, Authorization & Accounting via AdvOSS SDP scripting. This enables easy and flexible integration with external billing/charging systems in real time, thus enabling the CSP to seamlessly provide both Prepaid and Postpaid services.

It comes bundled with multiple applications to run behind the base RADIUS protocol front-ends. These Applications can be quickly and easily customized according to CSP requirements.

It also provides real time session management for ongoing user sessions.

There are many successful installations of AdvOSS AAA and it has been integrated with AAA clients embedded in servers from leading vendors including Cisco, Quintum, Juniper, Dialogic and others.



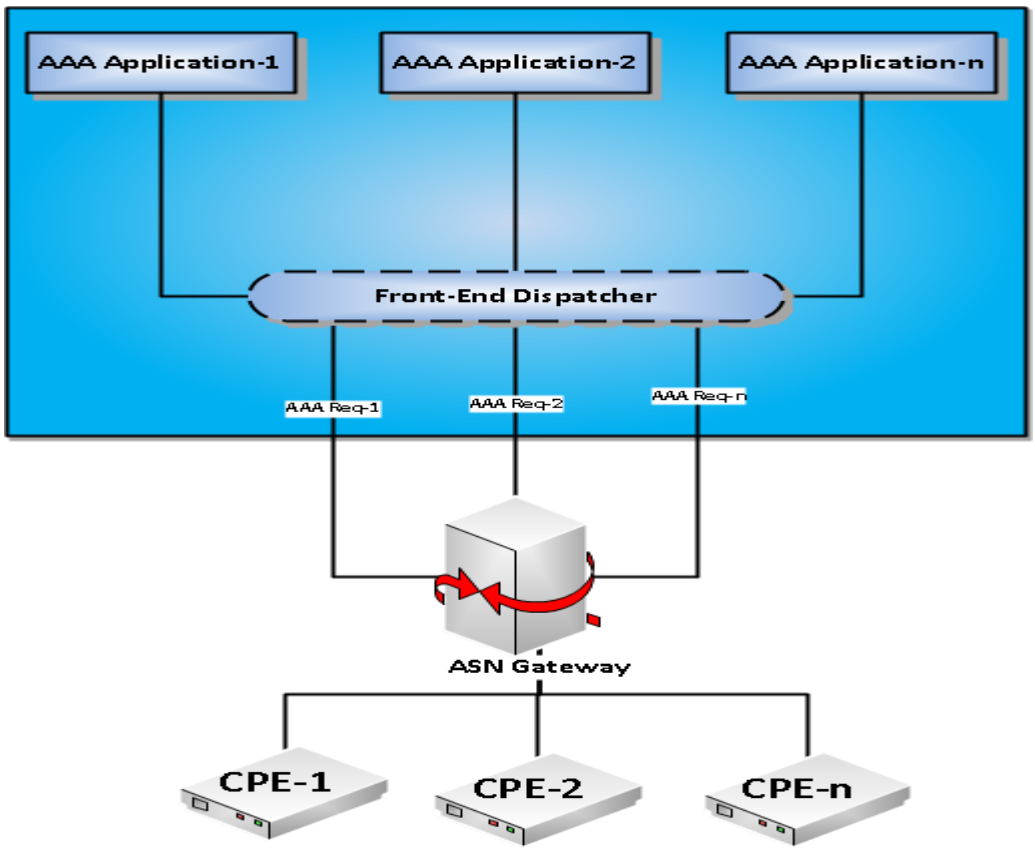

## 2 AAA Server's internal architecture

AdvOSS AAA is based on a highly scalable architecture.

The front-end of the solution is based on a protocol specific dispatcher e.g. RADIUS dispatcher, that performs some initial processing of the received AAA packet and distributes it in a highly efficient manner among a set of back-end AAA application instances performing load balancing. The back-end AAA application severs may be running on the same hardware machine as the front-end dispatcher, or on a separate hardware. The physical distribution of these applications is transparent to the front-end dispatcher because the dispatcher only deals with IP addresses and ports of the back-end applications.

This architecture allows maximum scalability within the limits of the front-end dispatcher. **The dispatcher shall be aware of whether the request is for EAP authentication or Authentication for Service Management based on NAS IP address.** It will forward the request to the target application (AAA) as appropriate.

## AAA Internal architecture diagram



# 3 Business Use Cases

- **Authentication**
  - Web based authentication
  - PIN based authentication
  - Automatic Authentication
  - PIN less authentication
  - PublicID based authentication
  - PrivateID based authentication
  - Device Authentication
  - Authentication for Nomadic & Mobile users
  - Identity theft & account sharing prevention
  - Lawful intercept
  - CPE sharing in corporate and multi-tanent environments
  - Unsubscribed user authentication for wifi hotspots
  - Integration with DHCP server
- **Service Profile (through HSS)**
  - Applicable bandwidth
  - Applicable QoS
  - Applicable personalization settings
- **Authorization**
  - Initial Authorization
    - Concurrency Authorization
    - Destination Authorization
      - Rating Engine
      - Parental Control
      - Phishing / Malware website server
      - Legally blocked destination server
    - Origin Authorization
    - Access Method Authorization
    - Access Number Authorization

        - Allowed time and usage authorization (through charging engine)
        - QoS authorization
        - Time of Day authorization
        - Session Management
        - Authorization of subscription
        - QOS & QOE authorization
        - Time of Day restrictions
        - Access Method control & charging
        - Authorization of multiple services
    - Re-Authorization
        - Monetary and Quota Re-Authorization through Charging Engine

- **Accounting**
    - Start Accounting
        - Monitoring interfaces
    - Interim Accounting
        - Real-Time charging through Charging Engine
    - Stop Accounting
        - CDR Writing
        - Refund of reserved counter and credit units
        - Sub-Invoice ID for CDR
        - Adjustment for Interim Accounting
    - Change of Authorization
        - Hot-lining
        - Change of service profile
    - Revenue Assurance Alerts
    - Service & Bandwidth control
    - Fair usage policies
    - Alerting
    - Redirections to self-care
    - Revenue Assurance

- QOS monitoring
- OTT Applications

# 4 Modules:

AdvOSS AAA is composed of the following main applications

- Authentication
- Authorization
- Re-Authorizations
- Start Accounting
- Interim Accounting
- Stop Accounting

AdvOSS AAA comes bundled with the following Applications

## 4.1 Authentication Application

### 4.1.1 Basic Authentication

- PIN
- CLI/ANI based
- Username/Password
- MD5 Digest Authentication
- IP based

### 4.1.2 Advanced Authentication

- **EAP Authentication** (RADIUS only)
  - EAP-TLS
  - EAP-TTLS
  - EAP-TTLS with MS-CHAP, PAP & MSCHAP V2
- IMS AKA

### 4.1.3 Interfacing with DHCP Server

AdvOSS AAA supports interfacing and integration with DHCP servers, thus abstracting out Authentication clients from DHCP details

- DHCP lease query

- DHCP address allocation request
- IP Address allocation and configuration via RADIUS attributes in Access Accept

For additional details about AAA Interfacing with DHCP Server please check knowledge base article from
http://www.advoss.com/resources/kb/AdvOSS-AAA-workflows.pdf

## 4.2 Authorization Application

- Authorization (Service & Service Profile)
- Authorization (Origin)
- Authorization (Request)
- Authorization (Concurrency)
- Authorization (Credit)
- Authorization (QoS)
- Authorization (Route)
- Authorization (Capacity)
- Others (Pluggable)

## 4.3 Re-Authorization Application

- Unit Reservation
- Quota Reservation

### Unit & Quota Reservation

- Units of duration or usage reserved by network service delivery function before delivering the service
- Units reserved from the account balance
- (Re-)Authorization application reserves the units before delivering service in collaboration with Charging Engine
- More units reserved when expired if session still going on
- Residual units returned to account from last reservation when session terminates
- Enables pure real-time prepaid behavior
- Enables concurrent sessions
- Account cannot go into negative balance ever

## 4.4 Accounting Application

- Start Accounting

- Interim Accounting
- Stop Accounting

## 4.5 Integration with Policy Server

For sending Policy based triggers / Change of Authorization (CoA) to clients

## 4.6 Session Management Module

It provides flexible session management for active user sessions

## 4.7 Concurrency Control Application

Configurable allowed concurrent sessions for each user.

## 4.8 Credit Control Application

Real time Authorization/Re-authorization via customizable workflows from external Rating & Charging Systems.

## 4.9 Service Control Application

Flexible service control via synchronous and asynchronous pushing of user service profile data to service enforcement points.

## 4.10 Logging

Configurable log levels for protocol requests and responses.

## 4.11 Staging Support

Configurable criteria to send selected requests to Backend staging server for predeployment testing and debugging.

## 4.12 Hunt-group based Routing

- User can create/Delete a new hunt group
- Specify users as members of Hunt-groups.
- Specify a RADIUS attribute as a filter to be used to match the Hunt-group in an incoming packet
- Associate IP address pools with Hunt-groups to bind specific users with specific IP address ranges. This feature is useful in controlling user access to the network from specific entry points only.

**Selective proxy and policy based routing**

User can specify an external AAA server if the packet contains a value in the Hunt-group filter attribute matching one of the members of the Hunt-group. This feature is useful in proxy-ing RADIUS authentication/authorization requests for specific users to other AAA servers for lawful intercept or similar reasons. For additional details about AdvOSS AAA Proxy Functionality please check http://www.advoss.com/resources/kb/AdvOSS-AAA-ProxyRole.pdf

## 4.13 Dynamic IP address allocation

AAA Server supports two types of dynamic IP allocation:

**NAS side pooling:**
In this case IP Pools are defined on the NAS side and IP addresses are assigned to those pools. The AAA Server selects a pool and returns its name in the Framed-Pool attribute to the NAS in Access-Accept response. Pools can be assigned to each user on the AAA server side in this case.

**Server side IP Pooling:**
In this case IP pools are defined on the AAA Server side and IP addresses are assigned to those pools. Each IP Pool is associated with a NAS client. When authentication request arrives from a NAS the AAA Server retrieves IP Pool associated with that NAS client. If successful, it selects and returns an unused IP address in the Framed-IP attribute in the Access-Accept response.

## 4.14 Subscriber Profiles Management

- **Local database**

  The solution shall have one instance of a local database for storing subscriber profiles and other provisioning data. This database will have a replicated peer on the other server. Both the peers shall be configured in a Master-Master replication mode. AdvOSS provides complete use cases for bulk and individual provisioning through its web-based Graphical User Interface (GUI) to populate data in the database. Data may include subscriber related information and

general configuration e.g. Hunt-group definitions, IP pool and policy based routing parameters e.g. third party AAA servers.

- **Subscriber profiles**

  The AAA solution shall maintain subscriber-related parameters in subscriber profiles in its locally attached database. These profiles shall be automatically replicated to the other peer DB instance on the other server. The profiles shall contain subscriber related information e.g. subscriber's MAC addresses, usernames/passwords, Hunt-group assignments and IP pool assignments (if any).

## 4.15 Management, Configuration and GUI

AdvOSS AAA server comes with a bundled web-server and database with a complete web-based GUI that provides role-based security, administrator groups and rights management for more details http://www.advoss.com/resources/kb/AdvOSS-AAA-Management-Configuration.pdf

## 4.16 SNMP Support

SNMP agent to interface with an external SNMP manager/NMS. The AAA Server supports SNMP based management by providing an embedded SNMP agent for monitoring and diagnostics of different parameters, through integration with external NMS.

## 4.17 Hot-lining Application (HLA):

The Hot-lining feature provides a Wi-MAX operator with the capability to efficiently address issues with users that would otherwise be unauthorized to access packet data services.

Hot-lining involves the Hot-Line Application (HLA). The Hot-Line Application performs the following roles:

- Determines when the user SHOULD be hot-lined. This requires integration with back-end billing and IN systems.
- Initiates the hot-lining signaling with the AAA.

- Responsible for initiating notification of the hot-line status to the subscriber. This could be done via a delivery of an HTML page to the subscribers' browser.
- Provides a mechanism for the user to rectify the issue that triggered hot-lining.
- Upon successful resolution of the problem, return the user back to normal operating mode.
- Upon unsuccessful resolution of the problem, terminate the user's packet data session.

**Hot-Lining Capabilities:**

A user can be hot-lined at the start of their packet data session or mid-session as described below:

**Active-Session Hot-lining:** The user starts a packet data session. In the middle of the session it is hot-lined and after the account is reconciled by some manner, the hot-lining status of the session is removed. The hot-lining is done with RADIUS Change of Authorization (COA) message.

**New-Session Hot-lining:** The user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session.

Similarly, hot-lined status can be removed mid-session or at the start of a new session.

There are two methods in which AdvOSS AAA indicates that a user is to be hot-lined:

**Profile-based Hot-lining:** The AdvOSS AAA sends a hot-line profile identifier in specific VSA in the RADIUS message. The hot-line profile identifier selects a set of rules that are pre-provisioned in the Hot-line Device (HLD) that cause that user's packet data session to be redirected and/or blocked.

**Rule-based Hot-lining:** The HAAA sends the actual redirection-rules (HTTP or IP) and filter-rules in the RADIUS messages that cause the user's packet data session to be redirected and/or blocked. These rules are sent to the NAS in specific RADIUS VSAs.

### 4.18 Captive Portal (Hot-Lining Portal):

AdvOSS AAA supports redirection of the users to a Web based Portal when a user is hot- lined.

Reasons for hot-lining a user are: prepaid users whose account has been depleted; or users who have billing issues such as expiration of a credit credit; or activate and signup the user.

AdvOSS Captive Portal provides web authentication portal for with self sign up and online payment process for the customers.

**Integration with Voucher Management System:** AdvOSS Captive Portal interfaces with Voucher Management System via an exposed API for voucher redemption.

## 5 Standards

| | |
|---|---|
| RFC 2138 | Remote Authentication Dial In User Service (RADIUS) |
| RFC 2139 | RADIUS Accounting |
| RFC 2865 | Remote Authentication Dial In User Service (RADIUS) |
| RFC 2866 | RADIUS Accounting |
| RFC 2869 | RADIUS Extensions |
| 3GPP2 P.S0001-B | cdma2000 Wireless IP Network Standard |

## 6 Integration Points:

AdvOSS AAA is based on standard Radius protocol for AAA and can be easily integrated with other B/OSS & Switching products to build larger

solutions. AdvOSS also has a range of B/OSS and Call Control products in its portfolio with which AdvOSS AAA comes pre-integrated as part of AdvOSS Solutions.

AdvOSS AAA offers points of integration with the following:

## 6.1 Front end:

AdvOSS AAA can integrate with any RADIUS compliant client including

- **Gateways/Softswitches**
- **Application Servers**
- **Routers, BRAS & Access Servers.**

It fully supports Vendor Specific Attributes (VSA) with the help of configurable XML based RADIUS vendor dictionaries. It also supports EAP Authentication schemes including EAP-TLS, EAP-TTLS and encapsulated EAP-TTLS protocols including MD5, PAP, CHAP etc.

## 6.2 Backend

On the backend, it can also integrate with the following

- **HSS (Home Subscriber Server)**
- **External Billing, Charging & Rating Engines**
- **External Databases** for Offline or Mediated Accounting
- **Locally Attached DB:**

  Option to create subscriber data for example authentication credentials in its locally attached database. This data can be provisioned using AdvOSS supplied API through an external provisioning System., and also AdvOSS provided web-based GUI. AdvOSS web-based GUI also provides bulk provisioning use cases for importing large subscriber data into the AAA database.

# 7 Key Technology Benefits:

AdvOSS AAA offers the following major benefits to the CSPs, in addition to its feature set:

## 7.1 Extensibility

AdvOSS AAA comes with the Scripting based workflow support (SCCXML & JAVASCRIPT).

AAA Applications are implemented as workflows. Workflows are implemented using Java script/XML therefore they are 100% customizable, extensible and modifiable. They are not customizable through pre-defined hooks or externally called script as is the case of most AAA vendors and competitors.

This also enables On the fly modifiability of the live system Using AAA workflows.

For additional details please check the knowledge base article from http://www.advoss.com/resources/kb/AdvOSS-AAA-workflows.pdf

## 7.2 Scalability

Built on top of AMPS middleware, AdvOSS AAA system provides very high scalability and can seamlessly scale to meet the requirements of medium size service providers to very large scale carrier grade telecoms.

AdvOSS has designed a Carrier Grade Scalability Architecture for unlimited throughput and number of subscribers by adding Hardware resources and Software application instances.

AAA Server is composed of a front-end protocol router/load balancer that acts as a Proxy for all NAS clients. It hides back-end AAA application servers e.g. EAP-TLS or EAP-TTLS applications.

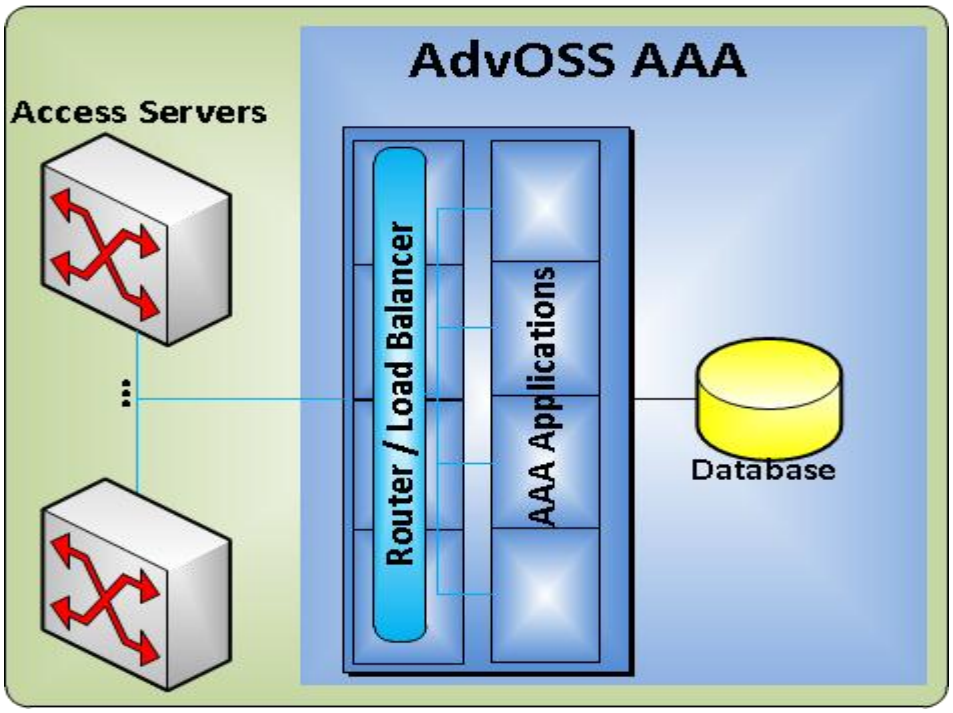
These back-end applications are also based on RADIUS or DIAMTER and the front-end router communicates with them internally, thus giving the illusion of a single server to the NAS clients.

The front-end Router is an efficient in-memory process that provides full proxy and load distribution functionality among multiple AAA Applications.

Each instance of Router is easily capable of handling up to 3**000 AAA** Transactions Per Second (TPS) running on a single CPU core for RADIUS/DIAMETER protocols whereas a single instance of AAA Application is capable of handling a minimum of **200 TPS.**

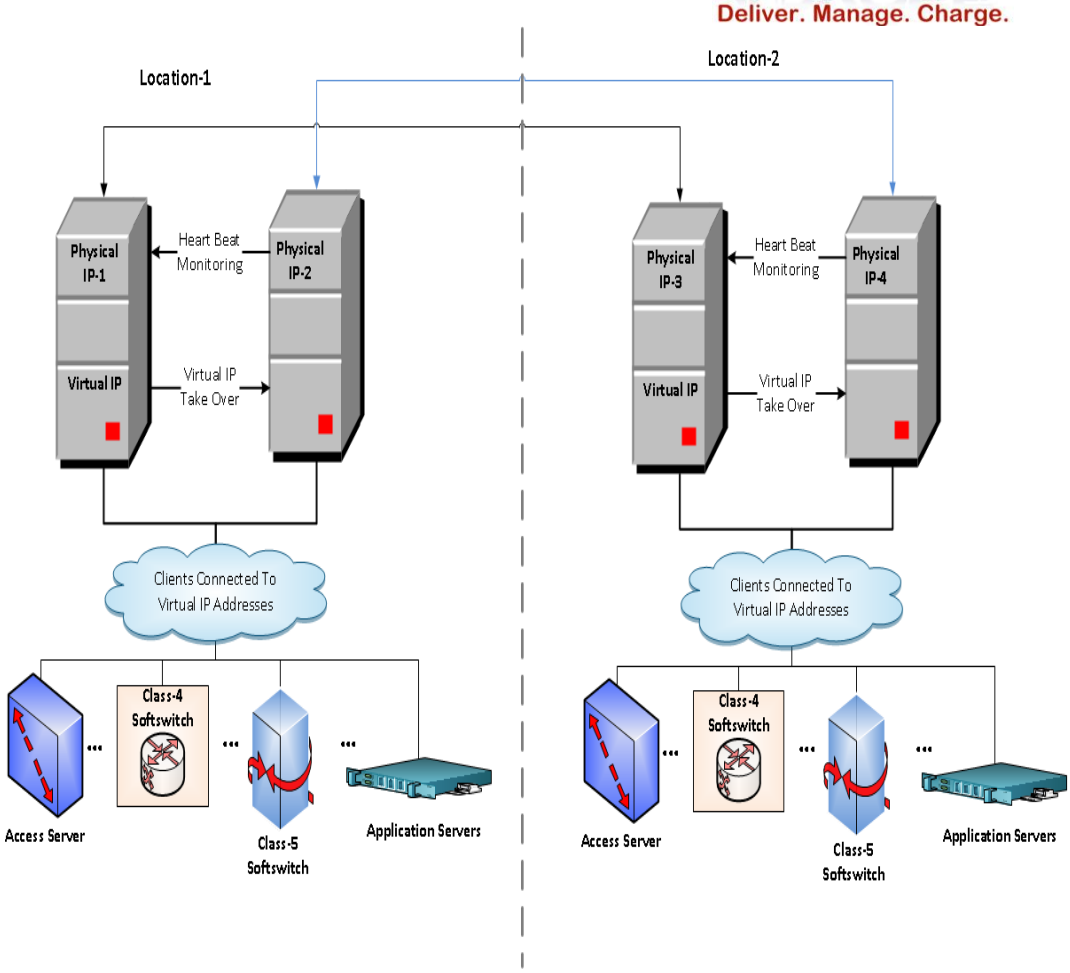
Thus on a high end server with 16 64-bit CPU cores and 16GB of RAM, AdvOSS AAA can easily handle between 2000 and 3000 AAA TPS.

For high end deployments, it is highly recommended that Database be deployed on separate servers so that database access can be scaled independently of the AAA application processing.




## 7.3 High Availability & Automatic Failover:

**System Level (1 + 1 redundancy)**
AdvOSS AAA supports a Virtual IP based high availability solution for 1+ 1 redundancy where it is primarily listening on a Virtual IP instead of physical IP.




The AdvOSS AAA provides a hot-standby server, along with an automatic failover and IP take over mechanism from primary to hot-standby in an order of a few hundred milliseconds. The primary AAA server in this case, runs on a virtual IP interface and a back-end additional IP interface to exchange heart-beat messages with its standby peer.
The hot-standby runs on the same virtual IP and another backend additional IP for communicating heartbeat with primary, but it keeps its virtual IP non-functional.

In the event that primary becomes non-reachable via heartbeats, the secondary brings its virtual IP up and running, and prepares itself immediately to receive new sessions on the virtual IP. The client applications, shall therefore, remain unaware of the switchover and shall keep sending request to the virtual IP.

### Local Monitoring Application

The AAA server has a built-in application process monitoring mechanism as a separate process.

If any application process comprising the solution ever crashes, it immediately restarts that process.

## 7.4 Geo-Redundancy

AdvOSS Hot IP takeover & automatic failover mechanism can also provide geo-redundancy among distant geographical sites if they are on same VLAN. If they are on separate LANs (or VLANs), then the AAA relies on NAS client's failover capability to send requests to the other geo-distributed sites if it does not receive timely responses from the primary AAA server.

This scenario is possible only when the both primary and its hot standby servers become unavailable i.e. the whole geographical site is not accessible from the NAS clients.

## 7.5 Failover (Database level)

AdvOSS AAA keeps a minimum of two database instances on two different machines acting as replicas of each other in Master-Master replication model. If one of the databases becomes unavailable, the AAA server automatically fails over to the other one for data read/write operations.

## 7.6 Congestion control at Database Level

AdvOSS AAA can be configured to throttle Database requests by configuring two parameters, high-watermark and low-watermark. Each AAA application keeps track of the Database queue where outstanding queries are placed. If the queue size increases beyond high-watermark, it stops queuing additional queries and goes into a Service Assurance state. When the queue size decreases below a low watermark (must be set to a value much less than the high-watermark), it resumes sending queries to the Database.

## 7.7 Robustenss

AdvOSS AAA can be configured to cache subscriber related data such as username/passwords and profiles in its local in memory cache to be able to serve customers in the face of Database unavailability.

This is an advanced mode and can be used for highly sensitive deployment scenarios where simple service assurance scenario of returning default service profiles is not desirable. In this mode, the AAA applications cache data on startup, and then update the data in memory on each successful query into the database. If the database ever goes unavailable, the local cache is used to serve

the requests. When the database becomes available again, the local cache updates are resumed and AAA resumes from the database.

## 7.8 Customizability:

AdvOSS AAA is highly customizable and can integrate with any AAA clients embedded in servers. It fully supports Vendor Specific Attributes (VSA) with the help of configurable XML based RADIUS and Diameter attribute definition dictionaries.

## 7.9 Disaster Recovery:

The System can be deployed in two geographically distant data centers, for disaster recovery reasons. It can also write Text based CDRs in local files for critical transactions that can be processed after last taken backup is restored to bring the DB to the most current state. Remote site database replication at the DR site is also supported.

## 7.10 Interoperability

AdvOSS AAA is interoperated and integrated with external HSS and Billing Systems such as Oracle BRM, Broadhop Subscriber Manager, Juniper Policy Server and others.

On the Network Access side, it has interworked with Motorola CAP-C, Huawei ASN Gateway, Cisco ISG, Cisco ASR, Alcatel Lucent ASN Gateway, Juniper BRAS, several Access Servers, Cisco BTS Class 5 Softswitch, NexTone Softswitch, Sonus Softswitch and others.

## 7.11 Flexibility:

The system is service agnostic and has the architectural provision to support any business model that may be a variant of pre-paid or post-paid or some hybrid of them. This allows for easy customizability to support specific requirements of a CSP.

## 7.12 Speed:

The system guarantees its claimed performance and speed of operations and latency times associated with the operations. AdvOSS AAA delivers 2000-3000 trans/sec on a single Intel Quad- core COTS server.

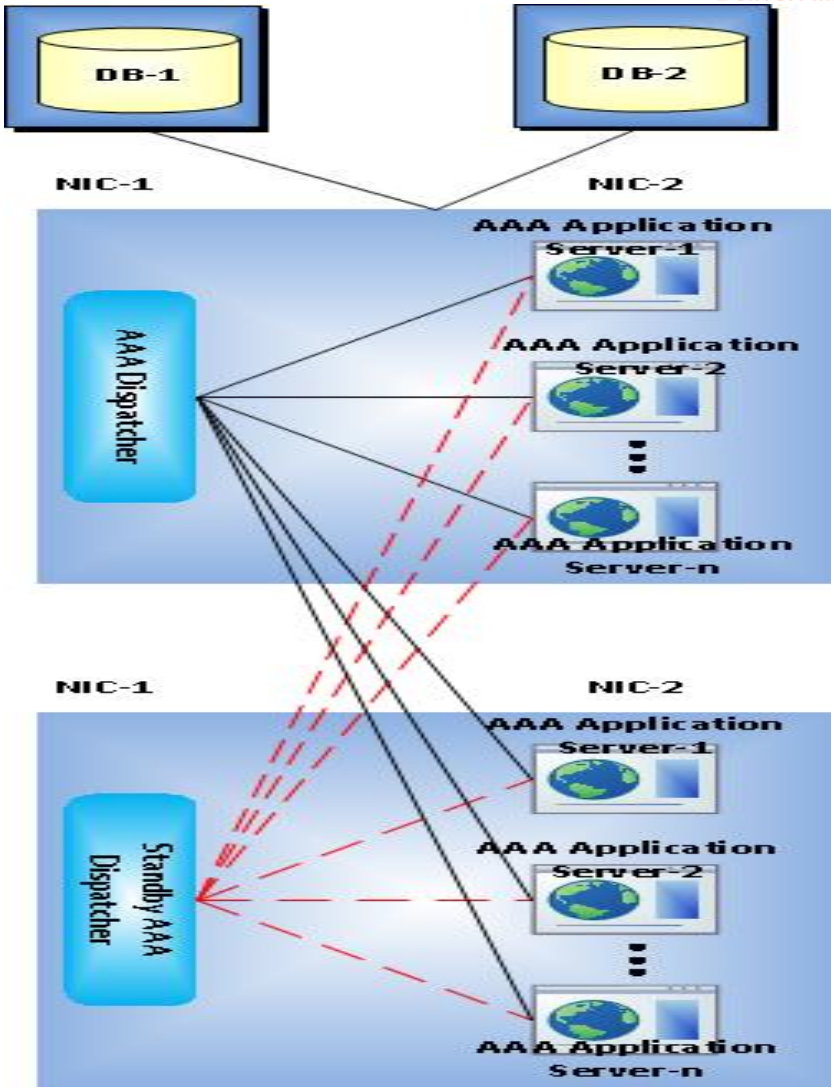
## 7.13 Security:

Security is implemented in the AdvOSS AAA at many levels.

- Administrative controls are implemented in GUI with full role-based security
- The administrative GUI maintains complete Audit Trail for provisioning operations.
- AAA requests can only be received from known NAS IP addresses.
- SNMP requests can be received from only known SNMP managers
- Integration with backend systems is through authenticated interfaces
- Passwords to back-end databases can be encrypted using public key authentication.

## 7.14 Resilience & HA model overview:

As mentioned earlier, AAA Server contains layer of Dispatcher and a separate layer of actual serving AAA Applications. Dispatcher is a stateless Proxy. The figure below shows a two server AAA solution.




As shown in the figures, there are two AAA servers and each server contains two network interface cards. Dispatcher 1 (main Dispatcher) is bound on NIC 1 on Server 1 whereas Dispatcher 2 (Standby Dispatcher) is also bound on NIC 1 on Server 2. AAA Application instances are bound on NIC 1 and NIC 2 at both servers.

**CASE 1: NIC 1 at Server 1 goes down**

- Dispatcher 2 takes over the IP
- New Traffic continues through standby Dispatcher 2 instead of Dispatcher 1

- Ongoing Traffic remains undisturbed as dispatcher is a state-less Proxy.

**CASE 2: NIC 1 at Server 2 goes down**

- New and Ongoing Traffic will continue as before without any change because AAA instances on server 2 are still accessible through the other NIC on server 2 (AAA Application instances are bounded on both NIC 1 and NIC 2 at both servers).

**CASE 3: NIC 2 at server 1 or server 2 goes down**

- New and Ongoing Traffic will continue as before without any change because AAA instances on server 1 or 2 are still accessible through the other NIC or server 1 (AAA Application instances are bounded on both NIC 1 and NIC 2 at both servers).

**CASE 4: Server 1 goes down due to a hardware or OS crash**

- Dispatcher 2 takes over the IP
- New Traffic continues through Dispatcher 2 and AAA instances on server 2.
- When server 1 becomes available again, the moved virtual IP goes back to server 1 automatically and traffic continues with full capacity as before

**CASE 5:Server 2 goes down**

- Dispatcher detects that AAA application instances on server 2 are no longs accessible. It stops sending traffic to them and uses only the instances running on its own machine.
- New traffic continues through server 1 only

- When server 2 becomes available again, dispatcher again detects this and starts distributing load on all instances of AAA across both machines

**Case 6:DB 1 instance goes down**

- Database queries shift to DB 2. Ongoing and new traffic will remain unaffected. If Database query queue size starts to increase, the AAA applications automatically switch to Service Assurance mode.

**CASE 7: Dispatcher Software Process crashes**

- Local monitoring re-starts it immediately (in the order of less than 30 seconds). Traffic will remain unaffected.

**Case 8: AAA Application software process crashes**

- Dispatcher detects that particular AAA Application instance has crashed i.e. no longer accessible and stops sending new sessions to that instance.
- Local monitoring re-starts the AAA application immediately. Traffic remains unaffected.
- When the process becomes available again, dispatcher again detects this and restarts sending traffic to that instance