AdvOSS High Availability Solution Architecture

Revisions

Version	Author	Date	Reviewed by	Comments
1.0	Fawad Pasha	June 15, 2011	Farhan Zaidi	Document Created

Introduction

This document High Availability Architecture which can be provided with a standard AdvOSS Billing & Switching Products deployment. This would include the following

- Conversion of all manual High Availability processes to Automatic Failover
- Monitoring Application
- Specification of HA model and methodology for all components as described later in the document

AdvOSS High Availability Architecture Description:

High availability shall be automatic, i.e. it would not require human intervention (almost) all cases. AdvOSS will provide a Monitoring Application to achieve automated High Availability.

1.1 Monitoring Application:

AdvOSS Monitoring Application shall have the following features

- Real time monitoring
- Heart beat management
- Virtual IP migration
- Application re-start on failure.

Monitoring Application will interface with Alerting app to send alerts or alarms. Monitoring can itself be monitored from the NMS as an Operating System process whereas for the applications monitored by the Monitoring Application, it will send alerts through alerting application (provided by AdvOSS), when any state change occurs.

High Availability will be achieved the in the following two ways:

1.2 Automatic failover from client side to a hot-standby

If the client served by an AdvOSS Billing & Charging component provides automatic failover capability in case a server does not respond to the initial request, the Billing would rely on the client to perform such failover. In this case the AdvOSS Billing will provide additional hot-standby server, configured on a separate IP address and running the replica of the primary application. To achieve this function, AdvOSS will add automatic switchover/failover with alarm logging/alerting modules in each component using this capability.

This model applies to the following components in AdvOSS Billing & OSS:

- **Billing & Charging Master Database**

Master database is accessed by the following data sources:

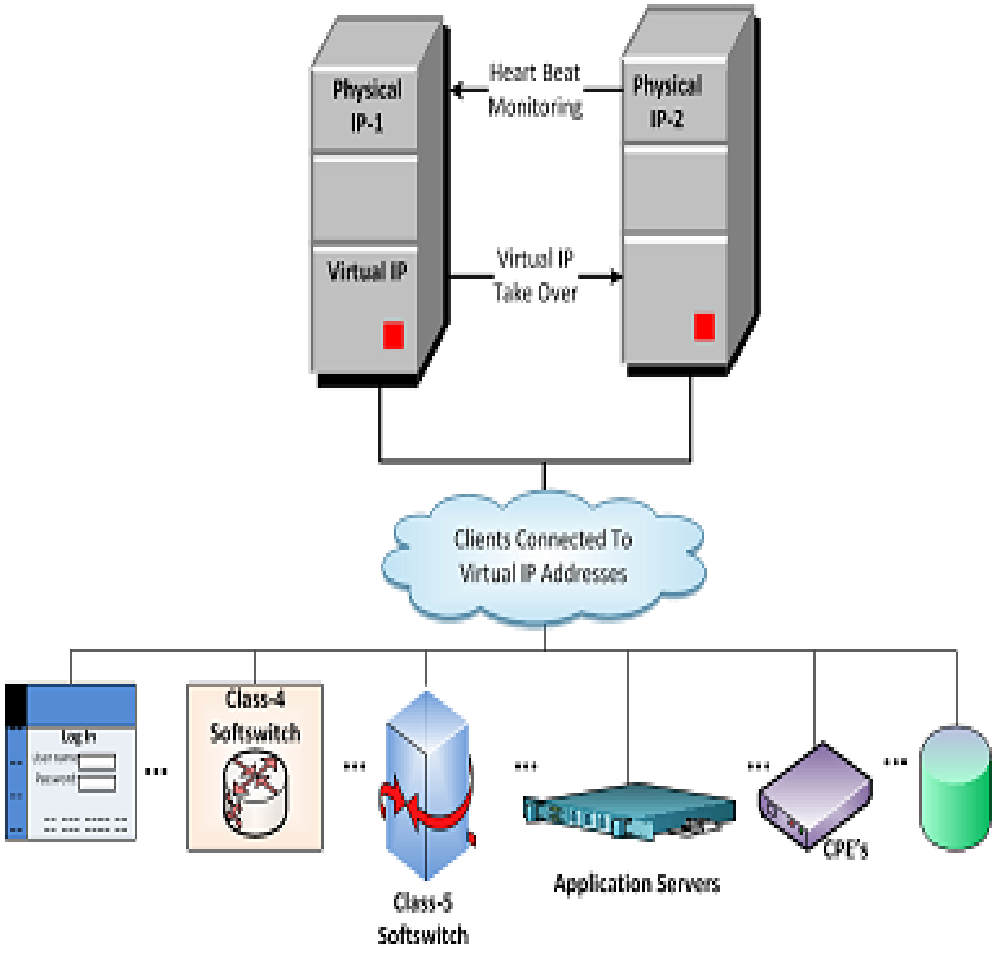
a. Billing administration GUI
b. CSR portals
c. AAA servers for voice and data

Each of these client components shall have the capability to perform failover to the secondary database in case of failure of the primary data-base access.

- **SIP Application Server:**
  Since, Class 4/class 5 switches that forwards the access requests to the SIP AS usually have the capability to perform automatic failover. A hot-standby server shall be added and SIP AS may use this capability of Class 4 /Class 5switch.

1.3 Automatic failover on server side using hot IP takeover

If the client served by an AdvOSS Billing & Switching component **does not** provides automatic failover capability in case a server does not respond to the initial request, then AdvOSS would provide 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 server in this case, shall run on a virtual IP interface and a back-end additional IP interface to exchange heart-beat messages with its standby peer. The hot-standby shall run on the same virtual IP and another backend additional IP for communicating heartbeat with primary, but it shall keep its virtual IP non-functional. In the event that primary becomes non-reachable via heartbeats, the secondary shall bring its virtual IP up and running, and prepare 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. The failover shall be transparent to them. To achieve this function, AdvOSS will add hot IP takeover / High Availability module with alarm logging/alerting modules in each component using this capability.



This model may applies to the following components:

- **AAA server**

  If any Application Server/Access Server deployed does not provide automatic failover capability, AAA Server shall utilize the hot IP takeover feature and failover to a secondary hot-standby in case primary AAA server goes down.

- **Admin GUI/CSR and Self-care portals**

  Clients of Billing Admin GUI and portals for CSR and self-care (web-browsers) usually do not provide any automatic failover capability to a secondary server. DNS round-robin can provide an alternative method of automatic failover but it

has issues regarding DNS timely updates and caching in clients, especially when components like Cisco ISG (Access Server) are involved in redirection and hot-lining of customers. Therefore, Billing shall utilize hot IP takeover for these components.

- **Provisioning server**

  Since clients of provisioning engine do not typically provide any automatic failover capability to a secondary server, therefore, Provisioning Engine shall utilize hot IP takeover for the provisioning engine.

- **IVR Application self-care**
  A hot-standby server shall be added during expansion for IVR self care and thus the two servers shall use this failover capability after expansion.

Note: If any external client component of AdvOSS Billing & Switching is not configured or does not have the capability to perform automatic switchover/failover then as a general principle, AdvOSS will use its Hot IP takeover/HA module to provide redundancy and fault tolerance to that component.