

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

IPWorks AAA Front End Function Overview

1	Introduction.....	2
1.1	Document History	2
1.2	Purpose.....	2
1.3	Scope.....	2
2	Overview.....	2
2.1.1	Solution Overview	2
2.1.2	Architecture.....	3
2.1.3	Data Model.....	4
3	LDAP Schema	4
4	AAA Front End Function.....	5
4.1	Data Query.....	5
4.2	Security Support	5
4.3	Load Sharing.....	5
4.4	High Availability	5
4.5	Result Code Behavior	8
4.6	Fault/Alarm Management	9
4.7	Performance Management	9
4.8	Data Provisioning.....	10
4.9	Cooperative Load Regulation	10
4.9.1	Early Traffic Rejection Procedure.....	10
4.9.2	Traffic Silent Discard.....	11
4.9.3	CUDB Node Failover	12
5	Call Flow	12
5.1	Generic Authentication and Authorization.....	12
5.1.1	PAP Authentication and Authorization	12
5.1.2	CHAP Authentication and Authorization	13
5.1.3	MSISDN Authorization.....	13
5.2	EAP Authentication and Authorization	13
5.3	PKI Authentication and Authorization.....	14
6	Operational Conditions.....	14
7	Standard Compliance Statement.....	14
8	Glossary.....	14
9	References.....	15

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

1 Introduction

1.1 Document History

Rev	Date	Sign.	Comment
B	2017-08-24	EMOYXIA/EJIAHLU	This document is of the first version.
B	2017-08-01	EJIOXUE	Refined the section 3, add section 5.3.

1.2 Purpose

The purpose of this document is to describe the AAA Front End functions supported by IPWorks.

1.3 Scope

This document mainly focuses on AAA Front End in which authentication and authorization parts of AAA functions cooperate with CUDB. Accounting is not included in this document.

2 Overview

This section provides a brief description of the AAA Front End (FE) supported functions.

AAA FE includes AAA FE (Radius) and AAA FE (PKI).

For AAA FE concept, see *IPWorks Technical Description*, [2].

2.1.1 Solution Overview

IPWorks AAA FE provides the connectivity with CUDB to get the user profile for Authentication and Authorization.

The AAA FE implements an application logic layer and provides the database query interface used to contact with CUDB by LDAP protocol. The AAA FE also provides failover and load sharing mechanism.

For details about IPWorks AAA, see *IPWorks Generic AAA Function Overview* [3], *IPWorks Wi-Fi AAA Function Overview* [4] and *IPWorks EPC AAA Function Overview* [5].

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

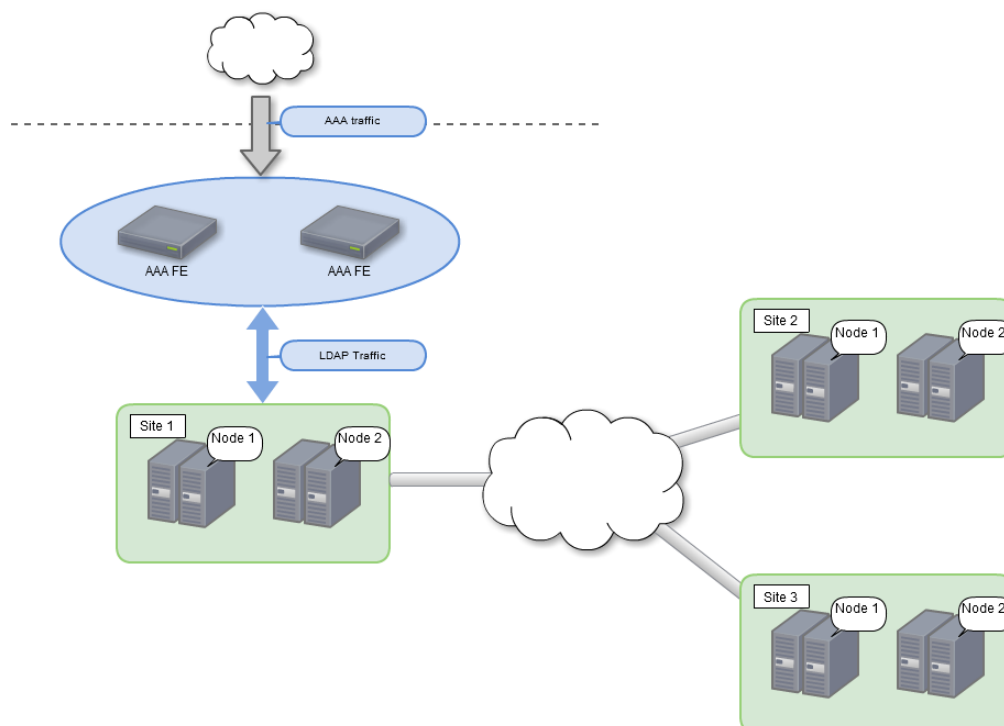


Figure 1 AAA Frond End with CUDB

Figure 1 shows AAA FE deployment with CUDB. CUDB is the redundant system deployed in different geographical areas to ensure the data accessibility. Data consistency is guaranteed by replication.

2.1.2 Architecture

IPWorks AAA FE is the component of Data Layered Architecture (DLA), where application and (user) data are separated in different layers, which are implemented in different network functional entities. The role of AAA FE is to provide the application logic and to enable AAA server to access CUDB instead of local NDB. CUDB is an extensible, high-performance, subscriber-centric database system, which communicates with IPWorks by LDAP protocol.

If AAA FE is enabled, AAA plays a role of LDAP client to query data from CUDB. For more details about LDAP protocol model, please refer to RFC 4511.

Figure 2 shows AAA Architecture in DLA. AAA FE acts as application layer while CUDB (the back end) acts as data layer. Data query request is sent by AAA FE and CUDB returns the result. Data provisioning is provided by Provisioning Gateway (PG). The connectivity between AAA FE and CUDB, CUDB and PG is based on LDAPv3 protocol.

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

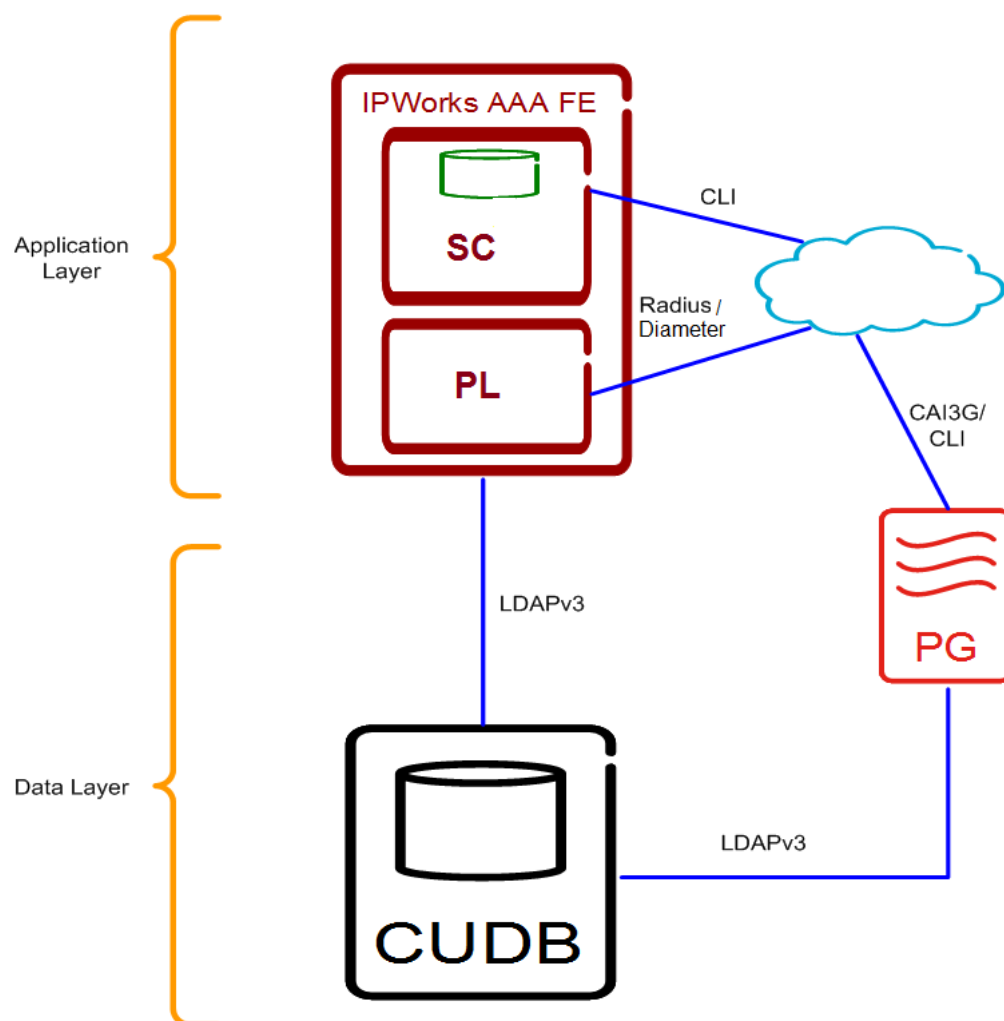


Figure 2 AAA Architecture in DLA

2.1.3 Data Model

The user data in CUDB is described as a Directory Information Tree (DIT). The tree is made up of entries that have names. One or more attribute values form the entry's relative distinguished name (RDN), which must be unique among its all siblings. The concatenation of the RDNs of the sequence of entries from an entry to an immediate subordinate of the root of the tree forms that entry's Distinguished Name (DN), which is unique in the tree. When AAA FE sends a query to CUDB, CUDB replies the AAA FE with entries including the user profile attributes according to the DN and filters.

3 LDAP Schema

This section provides details about user profile data stored in CUDB. For more information, refer to *IPWorks AAA LDAP CUDB Interface*, [1].

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

4 AAA Front End Function

4.1 Data Query

AAA FE uses LDAP protocol v3 to access CUDB for data query. TCP/IP is used as transport protocol on the physical interface towards CUDB nodes.

For details about LDAP search request and reply message, refer to RFC 4511.

4.2 Security Support

IPSec is supported for data traffic between CUDB nodes as well as between CUDB and AAA FE.

For details about IPSec, refer to RFC4301.

For IPSec configuration, refer to Configure Radius AAA [5]

4.3 Load Sharing

AAA FE supports multiple simultaneous LDAP connections in load sharing mode. The load sharing mechanism allows the AAA FE to distribute the needed capacity between two identical CUDB nodes and/or among several CUDB nodes.

When AAA server starts with CUDB support, AAA FE builds connections with all the CUDB nodes in the first site. The nodes in one site have the same priority. The connections are maintained in the connection pool.

AAA FE supports synchronous LDAP query. When querying data from CUDB, AAA FE obtains one connection from the connection pool for service and releases the connection to the pool after service request is responded from CUDB.

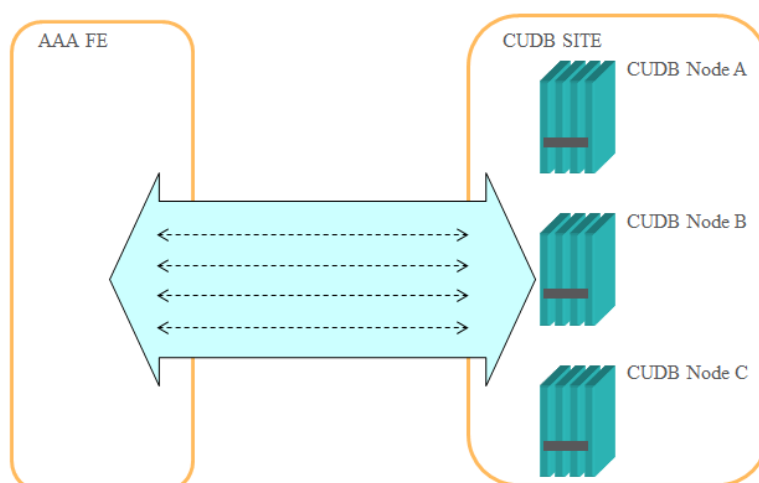


Figure 3 AAA FE Connection to CUDB Node

4.4 High Availability

CUDB is a high availability database, supporting geographical redundancy (several sites in different places) and node redundancy (several nodes in one site).

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

AAA FE supports CUDB site failover and fallback. AAA FE checks the connected status of the current site and the sites with higher priority at intervals by sending the CUDB polling request (LDAP Bind). The interval for check time could be configured (default value is 3 seconds). Failover and fallback is triggered at the checking interval.

If only parts of nodes in the site are down, the connections to the broken nodes are discarded at the checking interval. The broken connections are discarded when they are supposed to be used for data query. This mechanism is to speed up the connection release but could not trigger failover. The connections to these nodes are rebuilt in the coming checking interval if recovered.

Failover happens when all connections to the nodes of the current site are lost. Priority for CUDB site is configured by the order of the site IP configuration in the configuration file. AAA FE always tries to connect the higher priority site and does nothing to the lower ones. When site with higher priority is recovered, AAA FE triggers fallback in the coming checking interval. AAA FE rebuilds the connections to the higher priority site and then releases the connections to the current site. There should be no traffic lost during fallback.

The Figure 5 describes the scenario that AAA FE is running with site 1&2 down. The blue array means AAA FE is checking whether the site is recovered and red lines means there are connections. AAA FE is connected to site 3 currently and checking the connectivity of site 1&2.

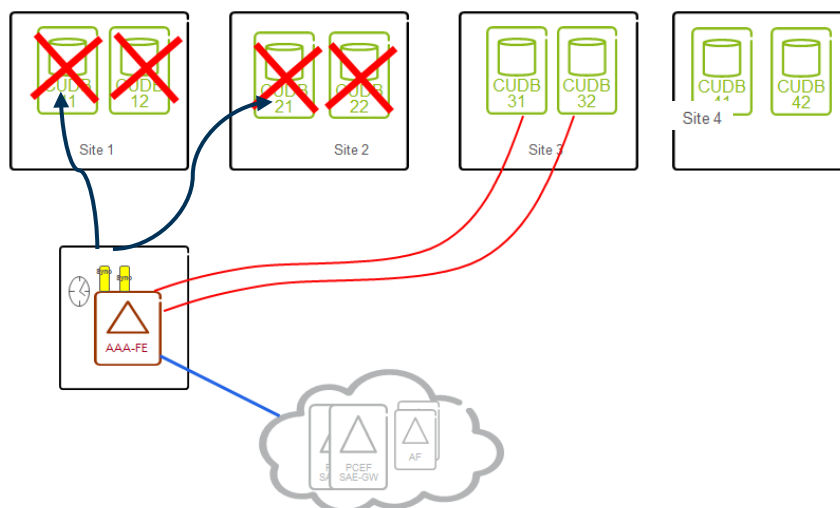


Figure 4 AAAFE with Site 1&2 Down

In the following figure, for example, CUDB is deployed with 1+1+1 geographical redundancy. When AAA server starts with AAA FE enabled, AAA FE builds connections with CUDB nodes in the first configured site.

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

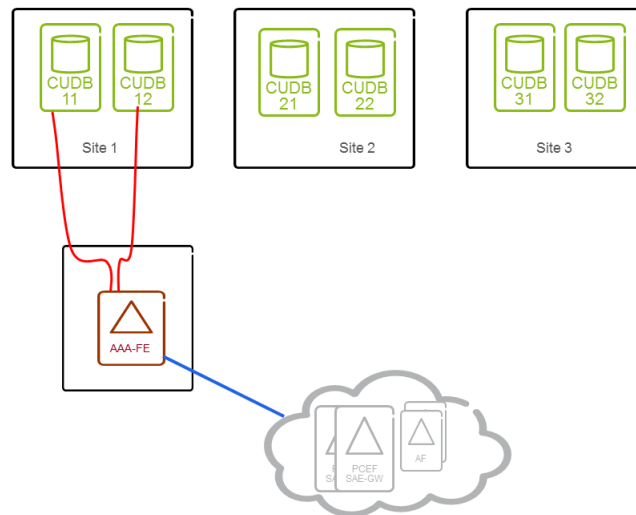


Figure 5 AAA FE with No Site Down

If one of the nodes in Site 1 is down, as Figure 7 shows, AAA FE will release the connections to the broken node. Failover are not triggered in this scenario. If there is data traffic, AAA FE will immediately detect node unavailable, release the connection used and re-distribute the request to other connection in the site; otherwise AAA FE will detect node unavailable and release all the connections to the broken node in the connection pool when checking site status at intervals. If the broken node is recovered, AAA FE will rebuild the connections when checking site status at intervals.

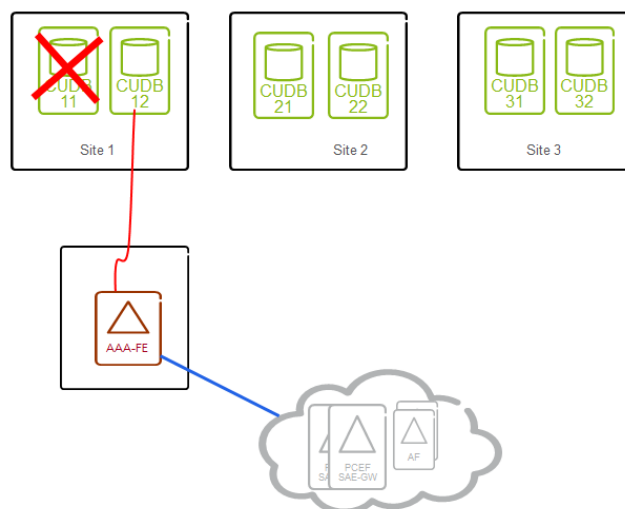


Figure 6 AAA FE Failover with One Node in Site 1 Down

In the following figure, if error occurs and all nodes in Site 1 are down, AAA FE connects to Site 2 for service failover. AAA FE checks whether Site 1 can be recovered at intervals as described in the beginning of this section. AAA FE would detect site unavailable and trigger failover when checking site status at intervals. Failover causes the traffic loss for a few seconds as there is time to detect the site is unavailable and to establish new connections.

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

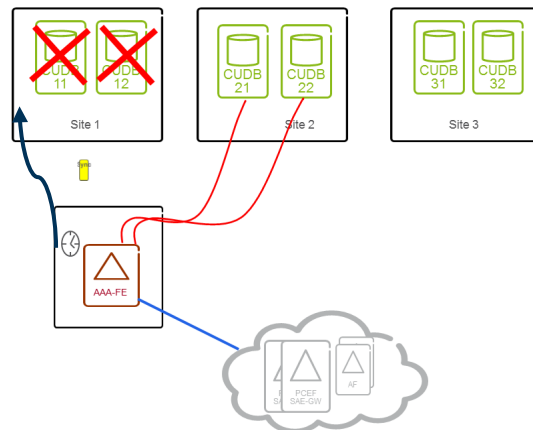


Figure 7 AAA FE Failover with Site 1 Down

When Site 1 is recovered, AAA FE falls back to Site 1. AAA FE builds the connections with site 1, and then releases the connections with site 2 (see the following figure). During the fallback, no traffic loss happens.

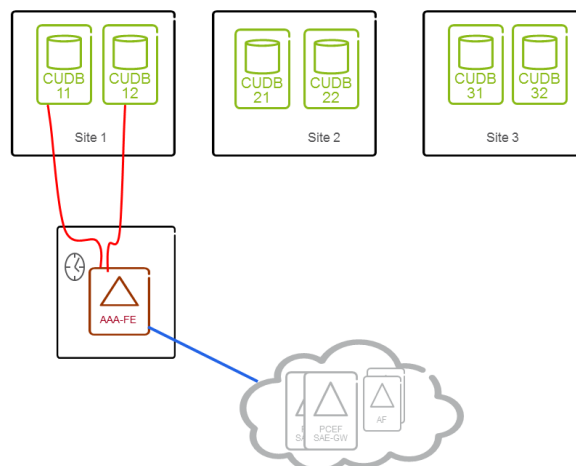


Figure 8 AAA FE with Site 1 Recovered

4.5 Result Code Behavior

This section describes the behaviors of AAA FE when AAA FE receives different result codes. Typical result codes are listed and others are considered as common error.

For details about CUDB result code, refer to CUDB CPI.

- Success (0): Indicates the successful completion. This is a non-error result code. AAA FE parses the returned entries into internal data structure. If error occurs in parsing, AAA server receives the error code INVALID_ARGUMENT (-5) and authentication fails.
- Busy (51), Unwilling to Perform (53), System Error (80): This error code indicates that CUDB is in an abnormal situation, for example, overload. No re-attempt is allowed and authentication fails when receive this error code.

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

- Unavailable (52): when receiving this error code, AAA FE would release the connection so the connection would not be used for query. Then AAA FE retries to query data using connections to other CUDB nodes in the same site. If this error is received at the checking interval, the connections to the nodes returning the error would be released. AAA FE triggers failover when receiving the error code from all CUDB nodes in the site at the checking interval (it means all the nodes in the site are down or unavailable). For details about failover, refer to Section 4.4. If no site works, the access-request query would be rejected with the reply/error message “authentication fails with Database service is unavailable” (or “DB not available for the user/id” for authorization). For more details about the work flow, please refer to section 5.
- Common Error (others): the access-request query would be rejected with the reply/error message “authentication fails with query failure” (or “unknown error for the user/id” for authorization). No CUDB failover when receiving the error code.

4.6 Fault/Alarm Management

AAA FE uses CBA FM Component for fault management.

Alarms include:

- Radius AAA, Server Cannot Connect to CUDB Node
- Radius AAA, Server Cannot Connect to CUDB Site
- Radius AAA, Server Entered CUDB Overload Protection
- Diameter AAA, Server Cannot Connect to CUDB Node
- Diameter AAA, Server Cannot Connect to CUDB Site
- Diameter AAA, Server Entered CUDB Overload Protection

For details about alarms, refer to *IPWorks Alarm List* [6].

4.7 Performance Management

AAA FE uses CBA PM Component for performance management.

Counters include:

- ipworksRadiusServTotalDiscardedCUDBQueryRequests
- ipworksRadiusServTotalCUDBQueryRequests
- ipworksRadiusServTotalSuccessCUDBQueryRequests
- ipworksRadiusServTotalFailedCUDBQueryRequests
- ipworksRadiusServTotalDiscardedLoadRegulationRequests
- ipworksRadiusServTotalCUDBErrorCodeBusyResponses
- ipworksRadiusServTotalCUDBErrorCodeUnavailableResponses
- ipworksRadiusServTotalCUDBErrorCodeOtherResponses
- ipworksDiameterServTotalDiscardedCUDBQueryRequests
- ipworksDiameterServTotalCUDBQueryRequests

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

- ipworksDiameterServTotalSuccessCUDBQueryRequests
- ipworksDiameterServTotalFailedCUDBQueryRequests
- ipworksDiameterServTotalDiscardedLoadRegulationRequests
- ipworksDiameterServTotalCUDBErrorCodeBusyResponses
- ipworksDiameterServTotalCUDBErrorCodeUnavailableResponses
- ipworksDiameterServTotalCUDBErrorCodeOtherResponses

For details about counters, refer to *IPWorks Measurement List*, [8].

4.8 Data Provisioning

AAA FE does not support data provisioning to CUDB. The data provisioning is implemented by Provisioning Gateway (PG). PG does not have any interface with IPWorks directly but CUDB, whereas, EMA is responsible for the provisioning in classic deployment by communicating with IPWorks through CLI interface.

For more information, please refer to PG documents.

4.9 Cooperative Load Regulation

IPWorks AAA FE supports graceful handling of overload condition by adapting to the cooperative overload protection mechanism introduced in UDC release. During the traffic handling procedure, IPWorks AAA FE can detect the CUDB overload status through receiving different error message from CUDB, and adopt different protection mechanism, such as early rejection of new incoming traffic and limiting traffic being sent in overload conditions.

4.9.1 Early Traffic Rejection Procedure

The external database (CUDB) is in an overload situation as a whole when it uses the Lightweight Directory Access Protocol (LDAP) error message LDAP_BUSY (error code 51) to warn the IPWorks about the inability to process all the traffic it is receiving.

IPWorks AAA FE evaluates the level of congestion in the CUDB according to the LDAP_BUSY response percentage from CUDB in a period. If the percentage is not beyond a threshold, which is configurable, AAA FE rejects the transaction that has failed with EC51 by silent discarding the received message, as below figure shows:

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

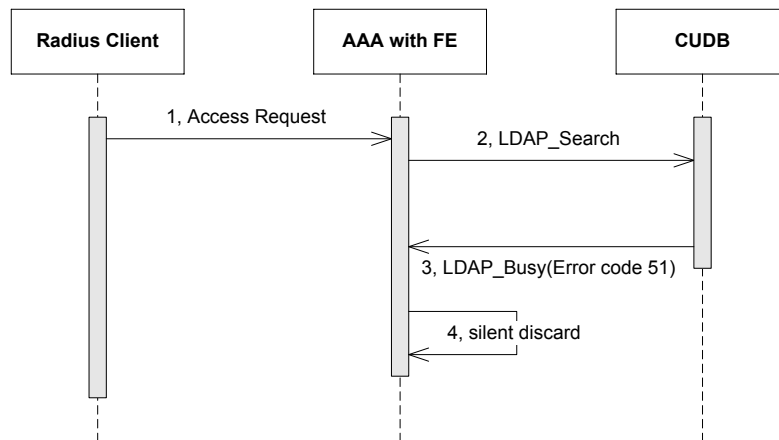


Figure 9 LDAP Busy Handling Procedure

When the error threshold is reached, the AAA FE starts performing early traffic rejection mechanism to silent discard part of incoming Radius traffics without processing. The abandoned traffic percentage increases if the LDAP_BUSY response is received continually in the next period. If the CUDB stop sending error code 51, AAA FE decrease the traffic discard percentage step by step until come back to normal.

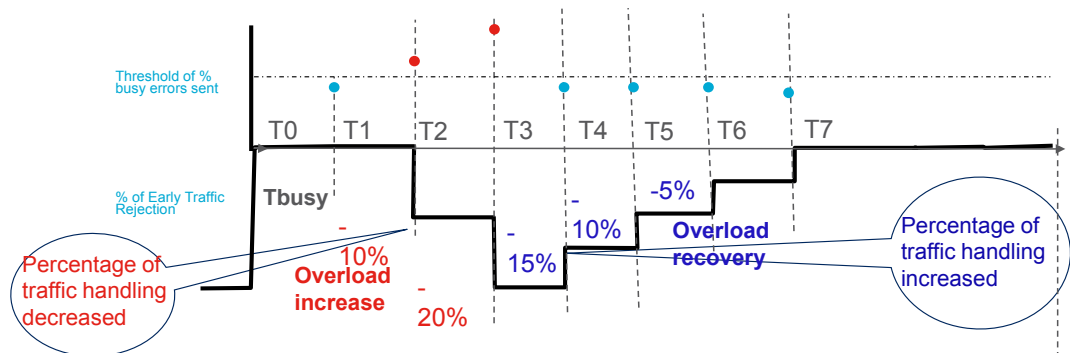


Figure 10 AAA FE Early Traffic Rejection Mechanism

An alarm is issued by the IPWorks AAA FE when early traffic rejection mechanism is activated. The alarm is cleared when AAA FE exits early traffic rejection mechanism.

4.9.2 Traffic Silent Discard

There are other kinds of overload situations in the CUDB that do not require any specific treatment by the AAA-FE. For example, the response with the error message LDAP_OTHER (error code 80) and LDAP_UNWILLING_TO_PERFORM (error code 53).

In this situation, the CUDB node is not considered to be overloaded as a whole, so AAA FE discards the message silently to avoid RADIUS client performing immediately and frequent reattempts when this error is received, and tries to slow down as much as possible application/network/terminal retry times.

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

4.9.3 CUDB Node Failover

If AAA FE receives LDAP response with error message LDAP_UNAVAILABLE (error code 52), AAA FE considers the CUDB node is not able to process new request for one of the following reasons:

- It has not enough available resources.
- There is a failure in a critical component within the CUDB node.

So, AAA terminates all the connections with this CUDB node and transfers all the other traffics to the other CUDB nodes.

At a specific interval, which is configurable, AAA FE tries to re-connect with the failed CUDB node periodically until the connections have been set up again.

5 Call Flow

This section describes the call flows between the AAA FE and CUDB. The call flow focuses on the message sequence to CUDB. Only the normal scenario, in which AAA FE queries data from CUDB, is described and Radius message is not detailed.

5.1 Generic Authentication and Authorization

This part focuses on the activity between AAA FE and CUDB in generic authentication and authorization scenario. For more information about the work flow, you can refer to [3]

5.1.1 PAP Authentication and Authorization

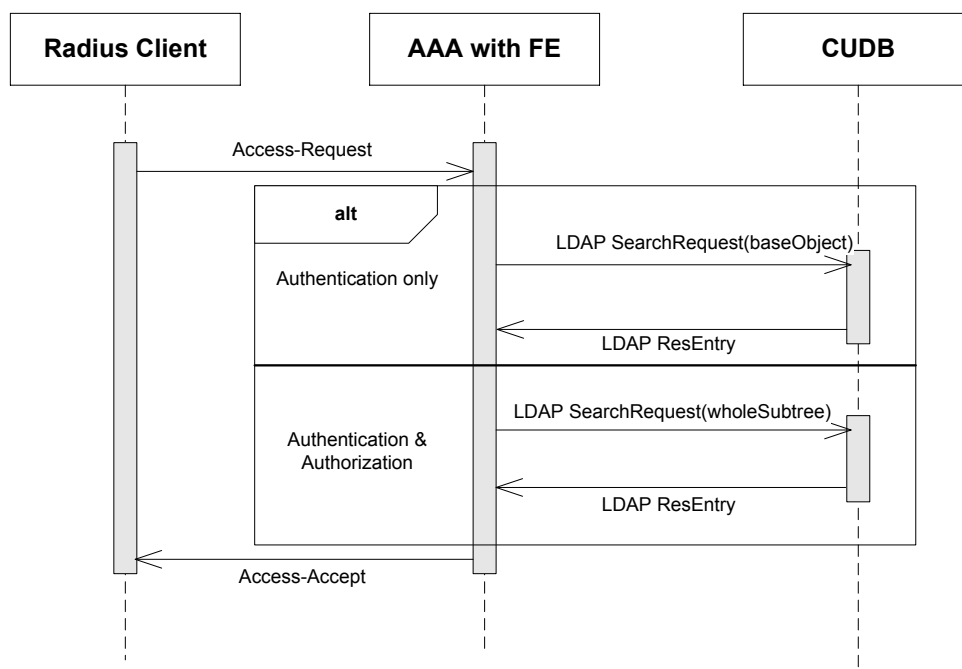


Figure 11 PAP Authentication with or without Authorization

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

5.1.2 CHAP Authentication and Authorization

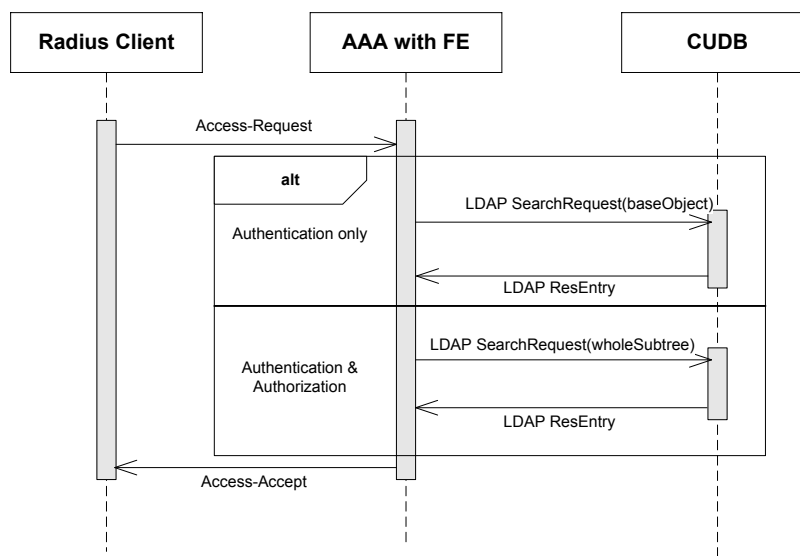


Figure 12 CHAP Authentication with or without Authorization

5.1.3 MSISDN Authorization

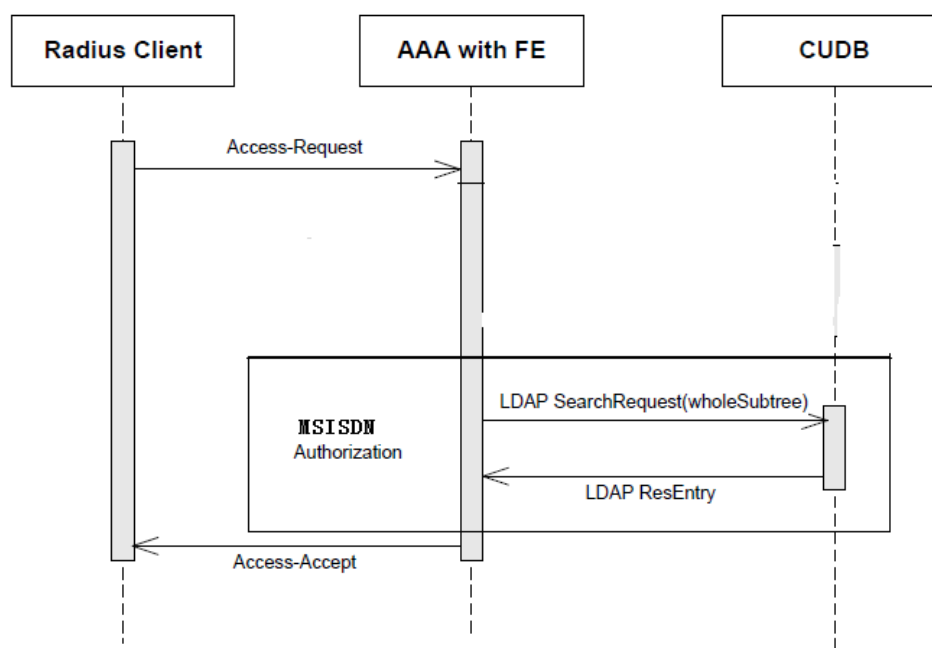


Figure 12 MSISDN Authorization

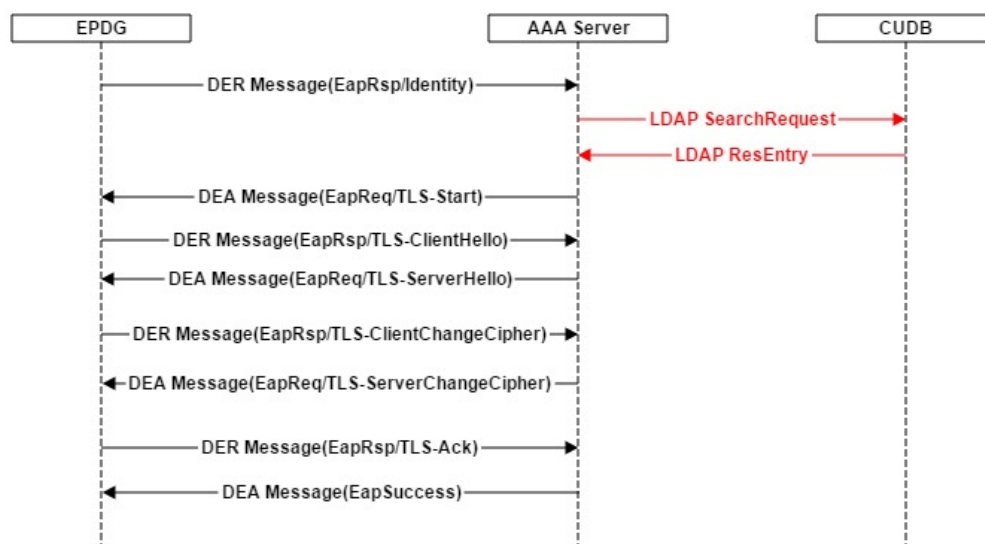
5.2 EAP Authentication and Authorization

This section focuses on the activity between AAA FE and CUDB in EAP authentication and authorization scenario in WIFI solution. For SIM based authentication (EAP-AKA/SIM), there were no direct connection between AAA FE and CUDB. For more information about the work flow, please refer to *IPWorks Wi-Fi AAA Function Overview*[4]

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

5.3 PKI Authentication and Authorization

This section focuses on the activity between AAA FE and CUDB in PKI authentication and authorization (based on EAP-TLS) scenario in Untrusted Non-3GPP IP Access Networks. For more information about the work flow, please refer to *IPWorks EPC AAA Function Overview*]



6 Operational Conditions

Refer to Section “Configuring AAA Front End (Radius)”, *Configure Radius AAA* [5]

Refer to Section “Configuring AAA Front End (PKI)”, *Configure EPC AAA* [7]

7 Standard Compliance Statement

- RFC4511 Lightweight Directory Access Protocol (LDAP)
- RFC4301 Security Architecture for the Internet Protocol

8 Glossary

AAA Authentication, Authorization, Accounting

CUDB Centralized User Data Base

DIT Directory Information Tree

DLA Data Layered Architecture

DN Distinguished Name

FE Front End

LDAP Lightweight Directory Access Protocol

NDB Network Data Base

Prepared (also subject responsible if other) EJIAHLU		No. 61/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

PG Provisioning Gateway

RDN Relative Distinguished Name

9 References

[1] IPWorks AAA LDAP CUDB Interface	24/155 19-AVA 901 16
[2] IPWorks Technical Description	221 02-FGC 101 3188
[3] IPWorks Generic AAA Function Overview	59/155 17-AVA 901 16
[4] IPWorks Wi-Fi AAA Function Overview	60/155 17-AVA 901 16
[5] IPWorks EPC AAA Function	57/155 17-AVA 901 16
[6] Configure Radius AAA	49/1543-AVA 901 33/2
[7] Configure EPC AAA	38/1543-AVA 901 33/2
[8] IPWorks Alarm List	2/006 51-AVA 901 33/2
[9] Fault Management	11/1551-AVA 901 33/2
[10] IPWorks Measurement List	3/006 51-AVA 901 33/2
[11] Performance Management	9/1551-AVA 901 33/2
[12] IPWorks EDA CLI Interface	51/155 19-AVA 901 16