

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

IPWorks Generic AAA Function Overview

Contents

1	Introduction.....	3
1.1	Document History	3
1.2	Purpose	3
1.3	Scope	3
1.4	Document Structure.....	3
2	Overview of AAA Functions	3
2.1	Overview.....	3
2.1.1	Architecture	5
2.1.2	Supported Functions	7
2.2	Actors	8
2.2.1	Actor: RADIUS Client (NAS).....	8
2.3	Sub-Functions	8
2.3.1	Authentication.....	8
2.3.2	Authorization.....	8
2.3.3	Accounting.....	9
2.3.4	IP Address Assignment	9
2.3.5	IPv6 Prefix Assignment	9
2.3.6	Proxy Server.....	10
2.3.7	Change-of-Authorization.....	10
2.3.8	Session Disconnect	10
3	AAA Functions.....	10
3.1	Authentication.....	10
3.1.1	RADIUS Authentication	10
3.1.2	PAP	12
3.1.3	CHAP.....	13
3.2	Authorization.....	14
3.2.1	RADIUS General Authorization	14
3.2.2	RADIUS MSISDN Authorization	15
3.2.3	Check List.....	16
3.2.4	Reply List.....	17
3.2.5	IP Address Assignment	18
3.2.6	IPV6 Prefix Assignment.....	19
3.3	Accounting.....	20
3.3.1	Accounting Session	22
3.3.2	Session Correlation	24
3.3.3	Session Management.....	26
3.4	Change-of-Authorization.....	27
3.5	Session Disconnect	27
3.6	Proxy Server.....	28

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3.6.1	Access/Accounting Message Proxy	29
3.6.2	DM/COA message Proxy	39
3.7	Overload Protection	42
3.7.1	Overload Discovery	42
3.7.2	Overload Control in Radius Backend	43
3.7.3	Message Discard under Overload	46
3.8	Authentication Support for Fixed Access IPoE	46
3.8.1	RB and BBF VSA	46
3.8.2	Fix Access IPoE Authentication.....	46
4	Operational Conditions.....	47
4.1	Configurable Parameters.....	47
4.2	Commands and User Procedures	47
4.3	Charging	47
4.4	Characteristics.....	48
5	Standard Compliance Statement	48
6	Miscellaneous	48
7	Terminology	48
7.1	Abbreviations.....	48
7.2	Definitions.....	48
8	References	49

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

1 Introduction

1.1 Document History

Rev	Date	Sign.	Comment
PA1-PA3	2017-04-01	ECIAMAO	First draft, based on 3/155 17-AVA 901 16 Uen L.
PB1	2017-06-09	ECIAMAO	Update the section 2.2.3 "Accounting".
PC1	2017-06-23	ECIAMAO	
PD1	2018-08-16	EZGUOZI	Add an new item in the table in section "2.1.1 Architecture".

1.2 Purpose

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

1.3 Scope

This document mainly focuses on the authentication, authorization and accounting of the AAA functions based on the RADIUS protocol. It will not cover all the network scenarios for the IPWorks AAA server.

1.4 Document Structure

2 Overview of AAA Functions

This section provides a brief description of the functions included in the AAA server.

2.1 Overview

The IPWorks AAA server provides Authentication, Authorization and Accounting functions for the wireline and wireless network access.

Authentication verifies the identity of an entity; Authorization determines whether a requesting entity is allowed to access a resource; and Accounting collects information on resource usage for the purpose of trend analysis, auditing, billing or cost allocation.

The IPWorks AAA server uses RADIUS as the traffic protocol to communicate with a Network Access Server (NAS), see the RFCs documents in the References section for more information.

Figure 1 displays a generic RADIUS scenario for IPWorks.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

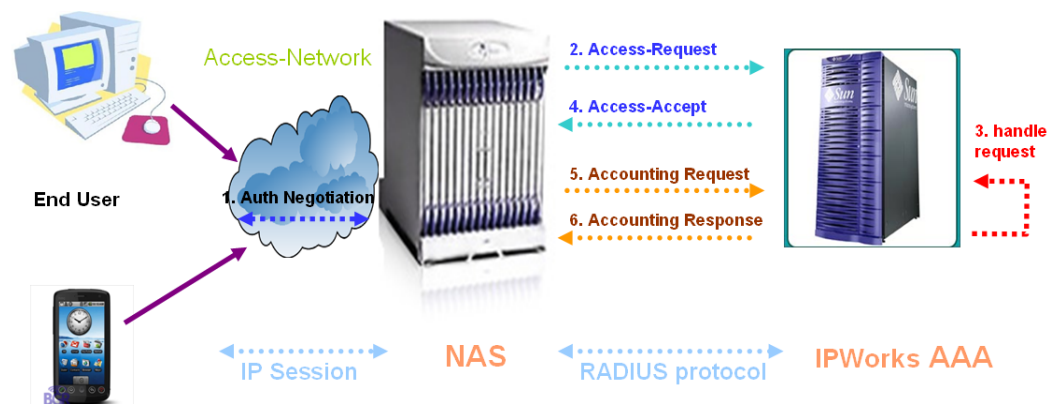


Figure 1 Generic RADIUS Scenario for IPWorks AAA

The following steps give a brief description of RADIUS messages exchanged between a RADIUS Client (NAS) and IPWorks AAA:

1. An end-user communicates with an NAS (referenced in Figure 1) through the access network. The authentication negotiation process takes place when the access procedure is starting. The end user may provide some authentication information (for example, user name and password) to identify itself.
2. The NAS then receives the user name and password or other authentication information, and creates an Access-Request message, to serve as the authentication request. It contains attributes, such as the user name and password, as well as the identity of the NAS.
3. Once an Access-Request message is received in AAA, it validates the NAS to see if it is authorized. If the NAS is valid, IPWorks AAA tries to find the user whose name matches the request and verifies its password. Additionally, users registered in AAA may be associated with a list of policies (Check List and Reply List) that must be fulfilled before access is granted.
4. If no policy is met for the incoming request, AAA sends an Access-Reject message, indicating that this user request is invalid (including a Reply-Message attribute pointing to the reason for failure), and the sequence terminates.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

When the user associated policy is met, AAA responds with an Access-Accept message. This message contains a list of attributes configured in the Reply List for that policy. ¹

5. At the start of service delivery, the NAS sends an Accounting-Request (Start) message. And during the service delivery, Accounting-Request (Interim-Update) messages may be sent.

At service completion, the NAS will send the Accounting-Request (Stop) message to the AAA Server.

6. After processing each Accounting-Request, IPWorks AAA replies with an Accounting-Response message.

2.1.1 Architecture

Figure 2 illustrates the architecture for the IPWorks AAA server. Under the default scenario, two service instances are used to achieve the traffic and data redundancy.

¹ As an exception, in WLAN AAA scenario, the related user information is not stored in AAA server. AAA server will try to get the user information from HLR and a uniform check list and reply list policy will be configured for all WLAN AAA users.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

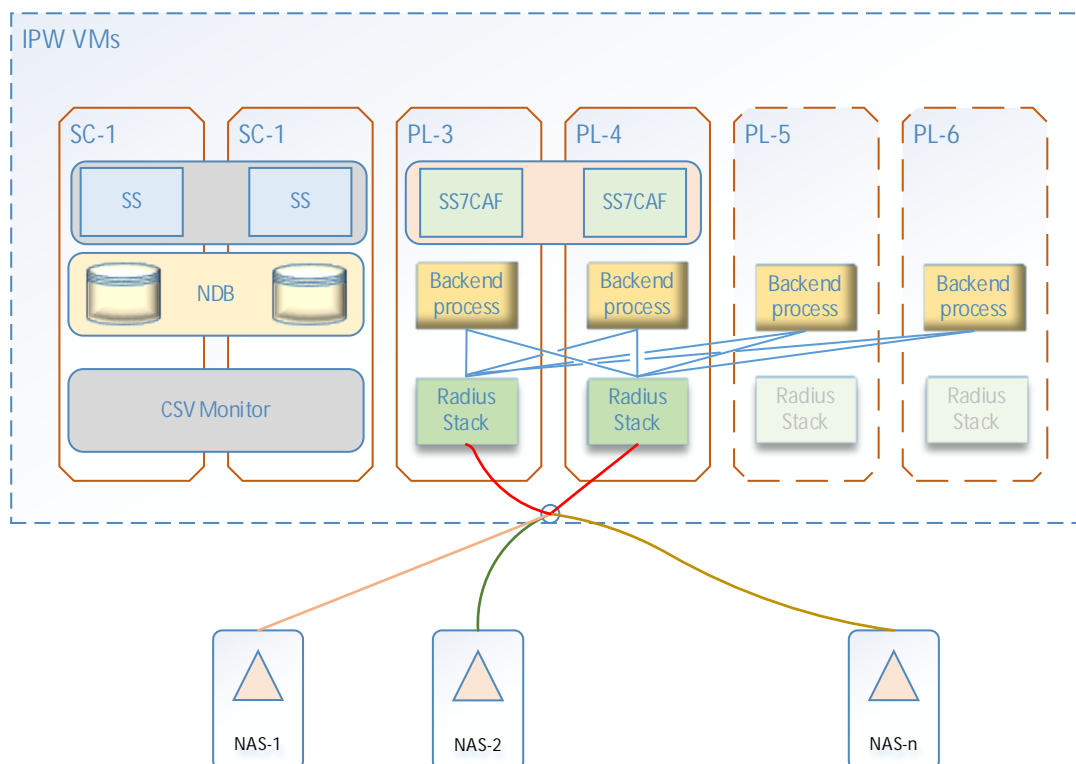


Figure 2 IPWorks AAA Server Generic Architecture

In IPWorks, the following functions can be triggered by the request type and AVP of the coming request:

- 1) Password Authentication Protocol (PAP)
- 2) Password Authentication Protocol (PAP)+General Authorization
- 3) Challenge-Handshake Authentication Protocol (CHAP)
- 4) Challenge-Handshake Authentication Protocol (CHAP)+General Authorization
- 5) MSISDN Authorization
- 6) Accounting

If the AVP(s) of the incoming request match the configured *triggerAVP* of a specified function, the corresponding function will be triggered. This trigger mechanism is called as selector logic. The *triggerAVP* of the specified function is configured through ECLI.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

If the message could match several different authentication methods, the highest priority (with lowest rank value) method will be executed. User can also specify if an authorization operation, which is based on local configured user policy, needs to be executed following the authentication method.

Below table shows the IPWorks default configuration for authentication selection mechanism. Authentication Method	Trigger AVPs	Rank	Need Authorization
EAP	"EAP-Message = *" "User-Name = *"	10	false
PAP	"User-Password = *" "User-Name = *"	20	Yes
CHAP	"CHAP-Password = *" "User-Name = *"	30	Yes
Pure Authorization	"User-Name = *"	40	false
msisdn-authorization	"User-Name = *" "Calling-Station-Id=*"	50	Yes

2.1.2 Supported Functions

The following figure shows the functions that are supported in the generic IPWorks AAA server. A detailed description is presented in the following sections.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

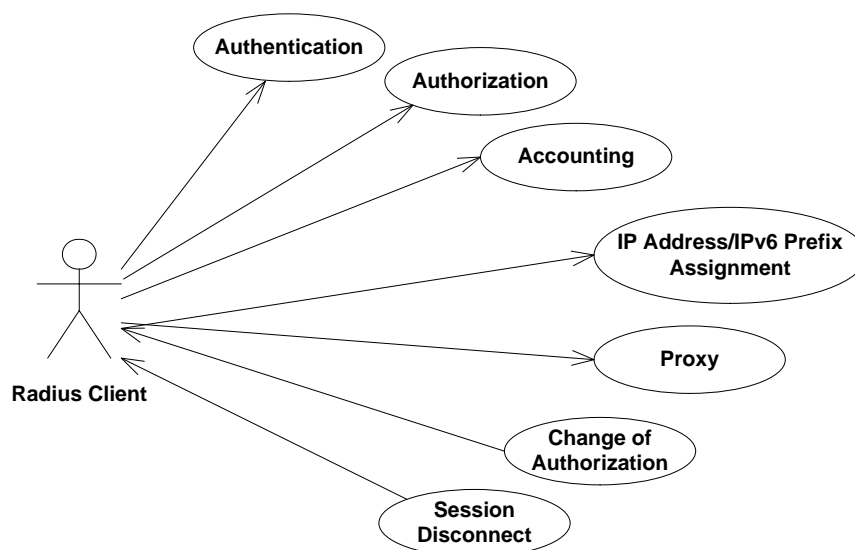


Figure 3 AAA Server Supported Functions

2.2 Actors

This section describes the actors involved in the AAA server.

2.2.1 Actor: RADIUS Client (NAS)

An NAS operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

2.3 Sub-Functions

This section describes the sub-functions of the AAA server.

2.3.1 Authentication

Authentication checks the identity of an entity trying to access a network. AAA Server verifies the entity by taking the specified authentication mechanism according to the authentication information provided in the request message. In IPWorks, the AAA server supports PAP and CHAP as the authentication mechanism in general AAA scenario.

2.3.2 Authorization

Authorization determines whether a requesting entity is allowed to access a resource. The AAA server authorizes the request by checking the preconfigured policy and including the corresponding attributes in the Access-Accept message according to the previous policy.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

2.3.3 Accounting

Accounting collects the resource usage for analysis or billing purposes. IPWorks AAA supports to generate a session-based accounting record or a message-based accounting record with the configured attributes received in the accounting messages and the configured built-in attributes. Using the message-based accounting record or the session-based accounting record is configurable.

Besides the general accounting functionality, AAA server introduces a new function so-called Accounting forward/mediation. The handling steps are as follows:

1. If the session function is enabled, a session will be created when the Access-Request message is authorized. When receiving accounting message, IPWorks AAA server handles the message locally based on the accounting session.
2. IPWorks checks the AVP list of the accounting message with the configured forwarding groups. For each forwarding group, if the AVP list value can match with the configured AVP trigger list and checklist in the forwarding group, IPWorks tries to forward the message to specified remote servers of the forwarding group.
3. During the forward procedure, IPWorks checks whether the accounting message includes Calling-Station-id and Framed-IP-Address AVPs, if not, IPWorks tries to insert these two AVPs for it using the value from accounting session.
4. After forwarding the message to all matched remote servers, IPWorks sends back the accounting response to client directly without waiting the response from remote servers.
5. If the remote does not response in time, IPWorks tries to resend the accounting message for several times and then gives up it. If the retry count is set as zero, then no resending action happens.

2.3.4 IP Address Assignment

IPWorks AAA can allocate an IP address for an authenticated user. The mechanism to allocate an IP address to a user can be defined in the user's profile.

2.3.5 IPv6 Prefix Assignment

IPWorks AAA can allocate an IPv6 prefix for an authenticated user. The mechanism to allocate an IPv6 prefix to a user can be defined in the user's profile.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

2.3.6 Proxy Server

The IPWorks AAA server can act as a proxy server between a RADIUS client (NAS) and the Home AAA Server. It forwards the authentication, authorization, accounting or other Change-of- Authorizations (CoA), and Disconnect messages to the corresponding target according to the configuration.

Proxy servers are commonly used for roaming.

2.3.7 Change-of-Authorization

If the user changes the authorization level, this may require authorization attributes to be added or deleted from a user session. In IPWorks AAA, a CoA message can be triggered to tell the NAS to modify the session authorization attributes.

2.3.8 Session Disconnect

IPWorks AAA provides the capability of notifying an NAS about the termination of a user accounting session. This is done by issuing Disconnect-Request messages to the NAS.

3 AAA Functions

This section provides a detailed description of the AAA functions.

3.1 Authentication

3.1.1 RADIUS Authentication

Authentication, authorization, or both, are performed in IPWorks AAA as a consequence of receiving a RADIUS Access-Request message. First, the IPWorks AAA server verifies that received RADIUS messages came from a neighboring node. Then, a password check is performed using the received password and the shared secret to perform an algorithm, and comparing it against the database. If the password is correct, authentication is successful. If the password is incorrect, authentication fails, and an Access-Reject message is sent by IPWorks AAA.

The RADIUS authentication methods supported by IPWorks AAA for password checking are PAP and CHAP. Which one to be used is selected based on the presence of either User-Password attribute or CHAP-Password attribute.

The authentication information is stored in the IPWorks database. Before a user is authenticated, the corresponding user information shall be provisioned in the IPWorks.

Error! Reference source not found. describe the general authentication process in IPWorks AAA.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

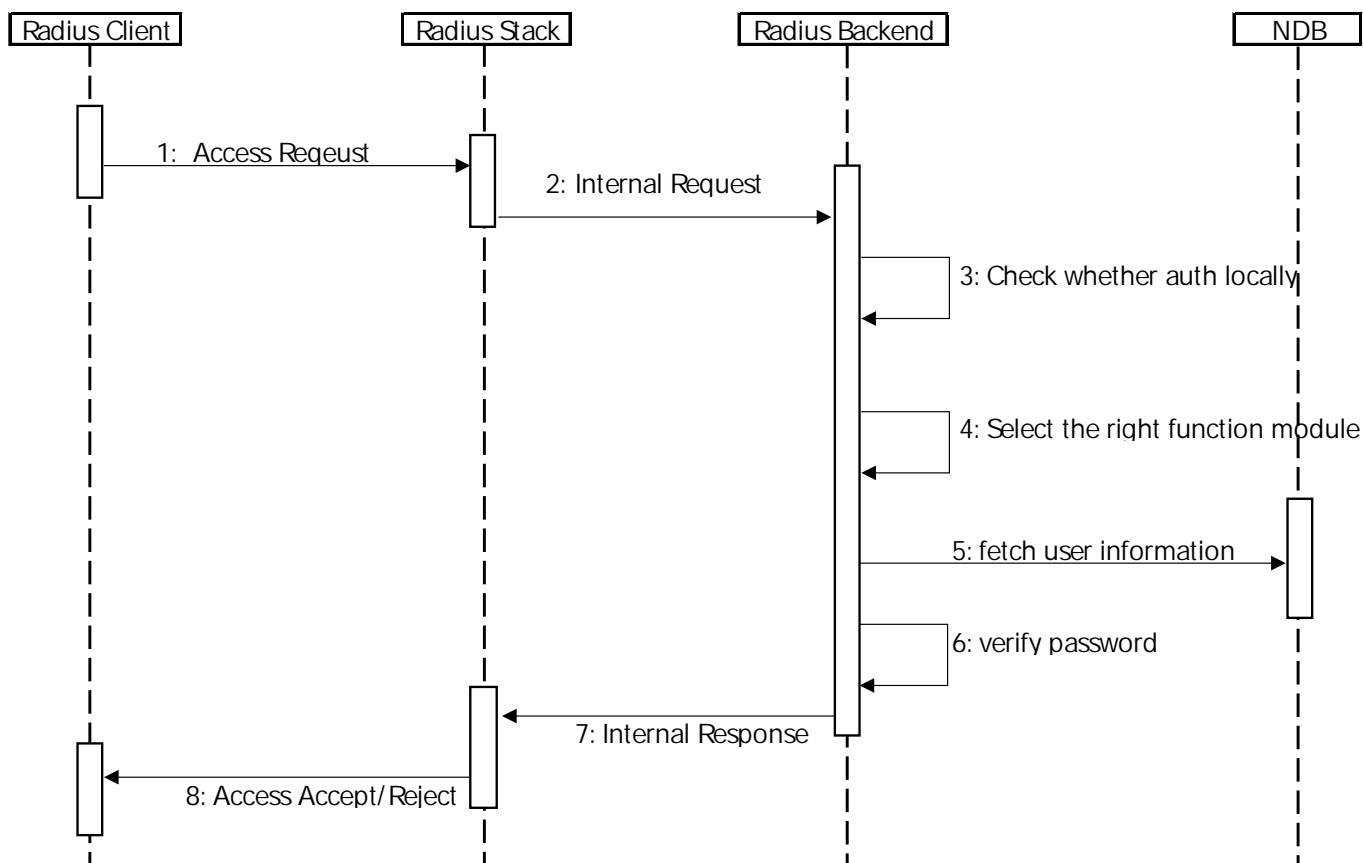


Figure 4 Authentication Process in IPWorks AAA

Note: To simplify the figure, the authorization steps have been omitted.

1. An Access-Request message is received by the IPWorks AAA server through the RADIUS stack.
2. The RADIUS stack decodes and validates the request message. If the request message is validated, an internal message containing the request information will be generated and sent to the AAA Backend.
3. The AAA backend checks the realm in the User-Name and determines if it shall act as a proxy to another AAA server according to the realm configuration. If the realm in the request matches the configured proxy realm, the Access-Request will be redirected to the corresponding target.
4. If the realm in the request does not match the configured proxy realm, the request will be sent to the authentication (PAP or CHAP) function module.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

5. The authentication function module fetches the user information from the NDB database according to the User-Name in the request.
6. A PAP or CHAP algorithm is taken to verify the access.
7. Regardless of whether the authentication is successful, an internal result response will be sent back to the RADIUS Stack.
8. The RADIUS stack is responsible for encoding the response and sending back the Accept or Reject message to the RADIUS client (NAS).

3.1.2 PAP

The PAP provides a simple method for the peer to establish its identity using a two-way handshake. For PAP, the NAS takes the PAP ID and password and sends them in the Access-Request message as the User-Name and User-Password. In IPWorks, the AAA server will trigger the PAP authentication algorithm when the User-Name and User-Password has been received in the Access-Request message. The function to be triggered is determined by the types of the request message and the Attribute Value Pairs (AVPs) in it. The operator can adjust the function trigger configuration according to the actual situation, although it is not recommended to change the default trigger.

Figure 5 displays the PAP authentication process.

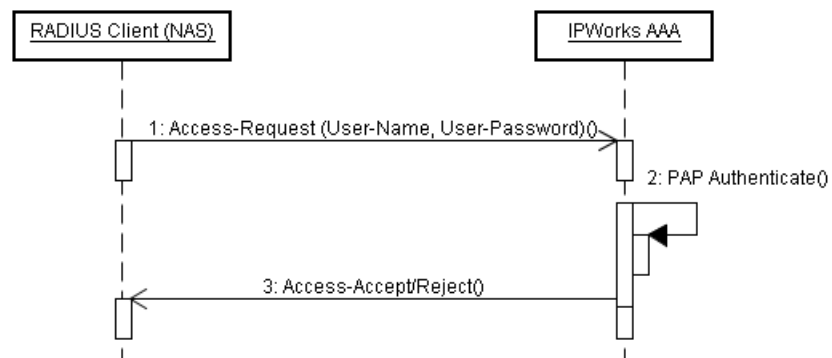


Figure 5 PAP Authentication

PAP is not a strong authentication method since there is no protection from a playback or repeated trial attack.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3.1.3 CHAP

CHAP is a more secure procedure than PAP. For CHAP, the NAS generates a random challenge and sends it to the user, whom then returns a CHAP response along with a CHAP ID and CHAP username. The NAS then sends an Access-Request message to the AAA server with the CHAP username as the User-Name and with the CHAP ID and CHAP response as the CHAP-Password. The random challenge can either be included in the CHAP-Challenge attribute or, if it is 16 octets long, it can be placed in the Request Authenticator field of the Access-Request message.

The IPWorks AAA server looks up a password based on the User-Name from the NDB, encrypts the challenge using MD5 on the CHAP ID octet, password, and the CHAP challenge (from the CHAP-Challenge attribute if present, otherwise from the Request Authenticator), and compares that result to the CHAP-Password in the request. If they match, the server sends back the Access-Accept, otherwise an Access-Reject message is sent back.

Figure 6 displays the CHAP authentication process.

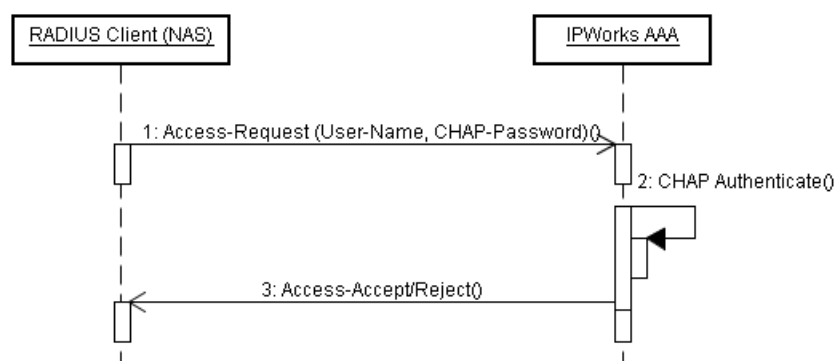


Figure 6 CHAP Authentication

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3.2 Authorization

IPWorks supports two types of authorizations:

- RADIUS General Authorization
- RADIUS MSISDN Authorization

MSISDN Authorization is a special authorization.

3.2.1 RADIUS General Authorization

The authorization phase can be triggered when an *Access-Request* message has been received and authentication procedure is finished.

Once the authorization is triggered:

- The AAA server checks if any user level policy exists, if no user level policy is found, the AAA server attempts to use the group level policies for the specified user.
- If no any policy is found from user policy and group policy, an *Access-Reject* is sent back to the client. If found, IPWorks AAA server will check the received packet attributes and values against the Check-Lists of policy for a user or user group. If the conditions of the Check-List are met, the IPWorks AAA server sets attributes in the *Access-Accept* message according to the corresponding Reply-List. Otherwise, the authorization fails and an *Access-Reject* message is sent back to the client.
- If more than one group policy has been matched, which means more than one Check List exists, the IPWorks AAA server always chooses the Check List with the maximum number of AVPs. This may lead to unexpected behavior, therefore, it is recommended to set mutually exclusive policies (Check Lists) for a user or a user group to avoid multiple hits on the Check List.

Figure 13 illustrates the relationship among the user, user group, and policy. A user can belong to several user groups, while multiple policies (Check List and Reply List) can be applied to a single user or a user group.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

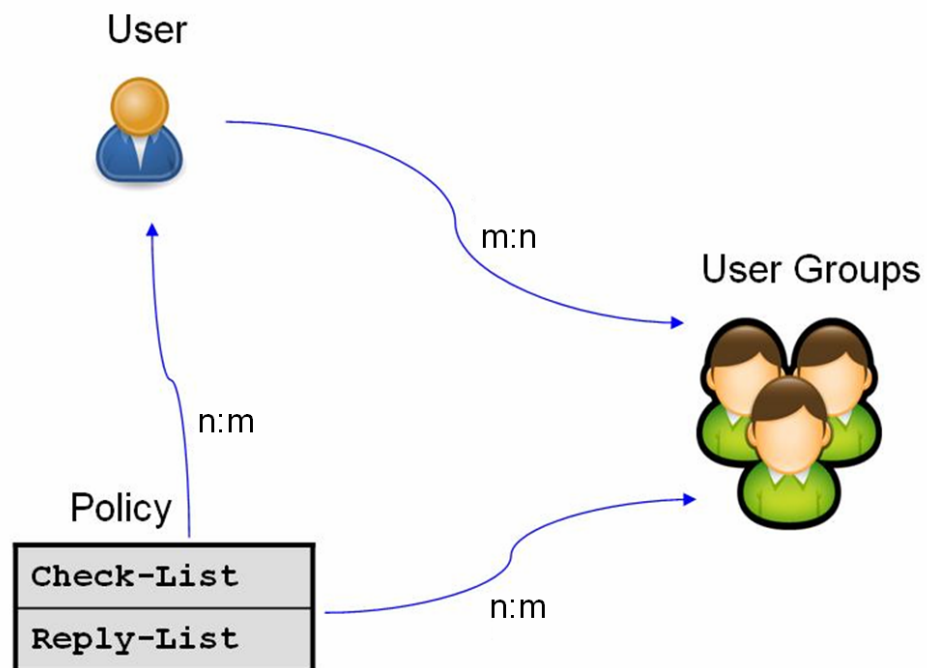


Figure 7 Relationship among User, Group, and Policy

3.2.2 RADIUS MSISDN Authorization

The authorization phase takes place when an *Access-Request* message has been received. The procedure is used to decide which attributes are to be included in the *Access-Accept* response message.

Once the authorization is triggered:

- The AAA server checks if any user level policy exists, if no user level policy is found, the AAA server attempts to use the group level policies for the specified user.
- If no any policy is found from user policy and group policy, an *Access-accept* message without any attribute is sent back to the client. If found, IPWorks AAA server checks the received packet attributes and values against the Check-Lists of policy for a user or user group. If the conditions of the Check-List are met, the IPWorks AAA server sets attributes in the *Access-Accept* message according to the corresponding Reply-List. Otherwise, an *Access-accept* without any attributes is sent back to the client.
- If more than one group policy has been matched, which means more than one Check List exists, the IPWorks AAA server always chooses the Check List with the maximum number of AVPs. This may lead to unexpected behavior, therefore, it is recommended to set mutually

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

exclusive policies (Check Lists) for a user or a user group to avoid multiple hits on the Check List.

3.2.3 Check List

The *Check List* is defined as a logical formula. If an Access-Request message fulfils the conditions of the complete formula, the Access-Request message is authorized.

The following items can be used in constructing the formula:

1. AVP Boolean expression, which supports the following operators:

Comparison operators

- > (greater than)
- >= (greater than or equal to)
- < (less than)
- <= (less than or equal to)
- == or = (equal to)
- != (not equal to)

>, >=, <, <=, == or =, and != is applicable for the attributes with an address or integer type. The AAA server only does the integer comparison when the ">, >=, <, <=" operators have been applied to the address type.

== or = and != are also applicable for an attribute with text and string type.

Conditional operators

- ? (the presence of the attribute)

? is applicable for any attribute, but only with value 0,1, and * ,

Attr ? 0: attribute does not exist;

Attr ? 1: attribute exist only once;

*Attr ? **: attribute exist more than once.

2. Logical operators for the expression combination: &&, ||.
3. Brackets ()

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

IPWorks AAA support many RFC standard attributes and vendor-specific attributes in the Boolean expression of the Check List. For the supported attributes in the Access-Request message, refer to [10] for more details.

In IPWorks, *System-Time* is a built-in attribute that represents the current time of the system. It allows the operator to control the acceptance of the requests within a specified time interval.

Example for the Check List

To authorize a RADIUS Access-Request message, the below conditions must be fulfilled:

The NAS-Identifier attribute is present (only once), no matter what value

and either:

the value of Service-Type attribute is "Login".

or

the value of Login-Service attribute is not "Telnet"

and

the system time is between 7:00 and 21:00 UTC.

Corresponding Expression:

`(NAS-Identifier ? 1) && (Service-Type = "Login" || Login-Service != "Telnet")
&& (System-Time > "7:00:00 UTC" && System-Time < "21:00:00 UTC")`

3.2.4

Reply List

If the *Check List* is matched, the corresponding *Reply List* will be used to set the attributes in the Access-Accept message.

A *Reply List* is a series of AVPs separated by commas. Please refer to IWD for IPWorks AAA Server and AAA Client [10] for the supported attributes in the Access-Accept message. The value of the attribute in the Reply List can be a constant static value or any attribute value that is present in the Access-Request message.

Example for the Reply List

A RADIUS Access-Request message has been authorized, and the following attributes will be replied to the client:

The NAS-Identifier which is same as the one in the Access-Request

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

and

*the MS-primary-DNS-server attribute with the value to be
"202.120.222.11"*

and Tunnel-Type with the value "L2TP"

Corresponding Expression:

`NAS-Identifier=$REQUEST, MS-primary-DNS-server="202.120.222.11",
Tunnel-Type="L2TP"`

3.2.5 IP Address Assignment

IPWorks AAA shall assign an IPv4 address to a user after a user is successfully authenticated. IPWorks AAA can assign IPv4 addresses to users in several ways:

- Static assignment —the same IP address is assigned to a user each time the user is authenticated successfully.
- Assignment from a specific address pool — an address is assigned from a specific pool when the user authenticated successfully.
- Assignment from pools associated with a RADIUS client — an address is assigned from one of the pools associated with the RADIUS client when a user authenticated successfully by the radius client.
- Assignment from pools associated with a RADIUS client based on APN selection — an address is assigned from one of the pools associated with the RADIUS client based on APN selection when a user authenticated successfully by the radius client.

The mechanism of IP address assignment can be defined in users' profiles.

IPWorks AAA treat the attribute "Framed-IP-Address" in the Access-Request as a hint for IP Address Assignment. IPWorks shall honor the IP address hint as the following description:

- If no mechanism of IP address assignment is defined in the user profile, "Framed-IP-Address" is used to select the IP address pool associated with the Radius Client. If the address is free, it can be allocated to the user; if it is not free, the next free address in the pool shall be allocated for the subscriber.
- If the mechanism of IP address assignment in the user profile is set to static assignment, the static address shall be allocated to the user.
- If the mechanism of IP address assignment in the user profile is set to assignment from a specific pool, if the Framed-IP-Address is already in the pool and free, the IP address can be allocated to the user; if the address is not included in the pool, or the address is not free, the next free address in the pool shall be allocated to the user.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- If the mechanism of IP address assignment in the user profile is set to Assignment from pools associated with a RADIUS client, if the Framed-IP-Address is already in a pool associated with the current Radius Client and free, the IP address can be allocated to the user; if the address is not included in the pool, or the address is not free, the next free address in the pool associated with the current Radius Client shall be allocated to the user.
- If the mechanism of IP address assignment in the user profile is set to Assignment from pools associated with a RADIUS client based on APN selection, if the Framed-IP-Address is already in a pool associated with the current Radius Client based on APN selection and free, the IP address can be allocated to the user; if the address is not included in the pool, or the address is not free, the next free address in the pool associated with the current Radius Client based on APN selection shall be allocated to the user.

If no appropriate IP address can be assigned to a user, IPWorks AAA shall let NAS to allocate an IP address to the user.

IPWorks AAA support IP pool HA feature with a cluster solution. The IP pool configuration and usage data shall survive from single point failure of SW and HW.

3.2.6 IPv6 Prefix Assignment

IPWorks AAA shall assign an IPv6 prefix to a user after a user is successfully authenticated. IPWorks AAA can assign IPv6 prefix to users in several ways:

- Static assignment —the specified IPv6 prefix is assigned to a user each time the user is authenticated successfully.
- Assignment from a specific IPv6 prefixes pool — an IPv6 prefix is assigned from a specific pool when the user authenticated successfully.
- Assignment from pools associated with a RADIUS client — an IPv6 prefix is assigned from one of the pools associated with the RADIUS client when a user authenticated successfully by the radius client.
- Assignment from pools associated with a RADIUS client based on APN selection — an IPv6 prefix is assigned from one of the pools associated with the RADIUS client based on the APN selection when a user authenticated successfully by the radius client.

The mechanism of IPv6 prefix assignment can be defined in users' profiles.

IPWorks AAA treat the attribute "Framed-IPv6-Prefix" in the Access-Request as a hint for IPv6 Prefix Assignment. IPWorks shall honor the IPv6 prefix hint as the following description:

- If no mechanism of IPv6 Prefix assignment is defined in the user profile, "Framed-IPv6-Prefix" is used to select the IPv6 Prefix pool associated with the Radius Client. If the IPv6 prefix is free, it can be allocated to the user; if it is not free, the next free IPv6 prefix in the pool shall be allocated for the subscriber.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- If the mechanism of IPv6 Prefix assignment in the user profile is set to static assignment, the static IPv6 Prefix shall be allocated to the user.
- If the mechanism of IPv6 Prefix assignment in the user profile is set to assignment from a specific pool, if the Framed-IPv6-Prefix is already in the pool and free, the IPv6 Prefix can be allocated to the user; if the IPv6 Prefix is not included in the pool, or the IPv6 prefix is not free, the next free IPv6 Prefix in the pool shall be allocated to the user.
- If the mechanism of IPv6 prefix assignment in the user profile is set to Assignment from pools associated with a RADIUS client, if the Framed-IPv6-Prefix is already in a pool associated with the current Radius Client and free, the IPv6 prefix can be allocated to the user; if the IPv6 prefix is not included in the pool, or is not free, the next free IPv6 Prefix in the pool associated with the current Radius Client shall be allocated to the user.
- If the mechanism of IPv6 prefix assignment in the user profile is set to Assignment from pools associated with a RADIUS client based on APN selection, if the Framed-IPv6-Prefix is already in a pool associated with the current Radius Client based on APN selection and free, the IPv6 prefix can be allocated to the user; if the prefix is not included in the pool, or the prefix is not free, the next free prefix in the pool associated with the current Radius Client based on APN selection shall be allocated to the user.

IPWorks AAA support IPv6 prefix pool HA feature with a cluster solution. The IPv6 prefix pool configuration and usage data shall survive from single point failure of SW and HW.

3.3 Accounting

Once the access has been granted to users, accounting information related to the user or session may arrive at the AAA server (up to the configuration of the NAS).

The IPWorks AAA Server collects the accounting information by recording the received attribute values as the CSV file. The attributes value to be recorded can be configured in the CLI. The IPWorks AAA Server support to generate message-based accounting CSV files and session-based accounting CSV files.

Figure 8 displays the message-based accounting process used in IPWorks AAA.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

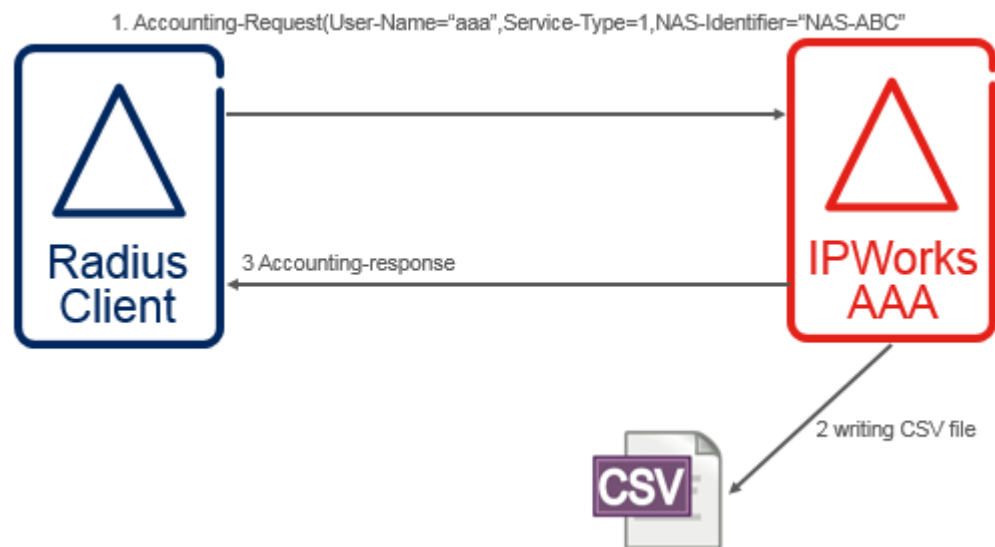


Figure 8 Message-based Accounting Process in IPWorks AAA

Figure 15 displays the session-based accounting process used in IPWorks AAA.

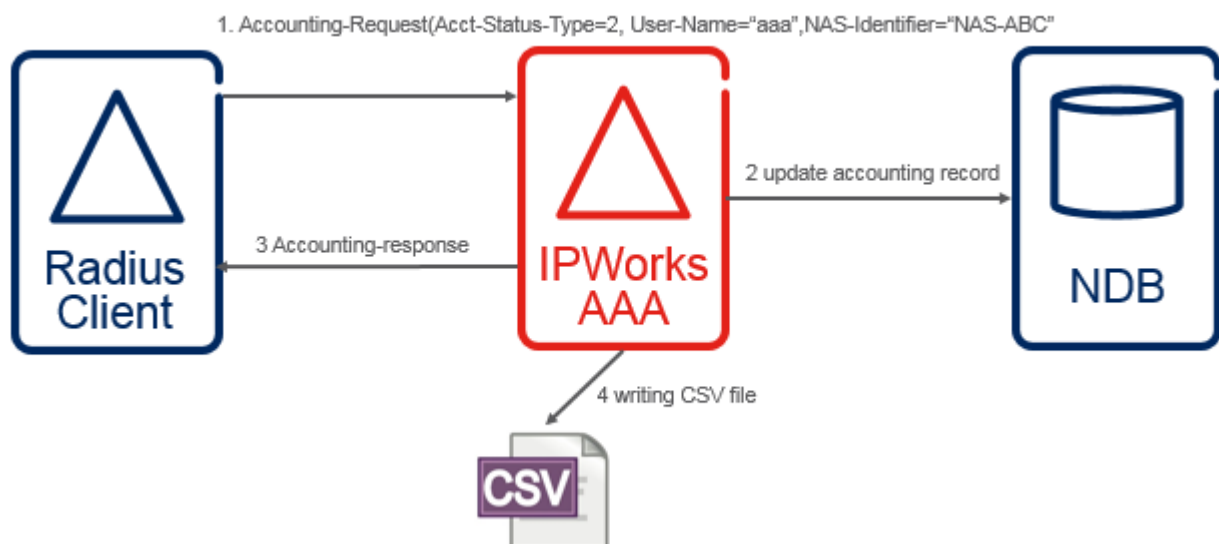


Figure 15 Session-based Accounting Process in IPWorks AAA

A new accounting CSV file will be created by following the rule according to any of the four principles:

- The size of the CSV file reaches the configured size;
- The record number of the CSV file reaches the configured number;

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- The time range (since the file was created) of CSV file reaches the configured time interval;
- CSV file reaches the configured file size or the time range reaches the configured interval;

3.3.1 Accounting Session

If the session function has been enabled, a Session will be created when the Access-Request message has been authorized. This Session enters the active status when the first Accounting-Start message is received and ended with the reception of the corresponding Accounting-Stop message or by maintenance procedures (Session Disconnect).

Figure 6 shows the condition that causes the session state to be changed.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

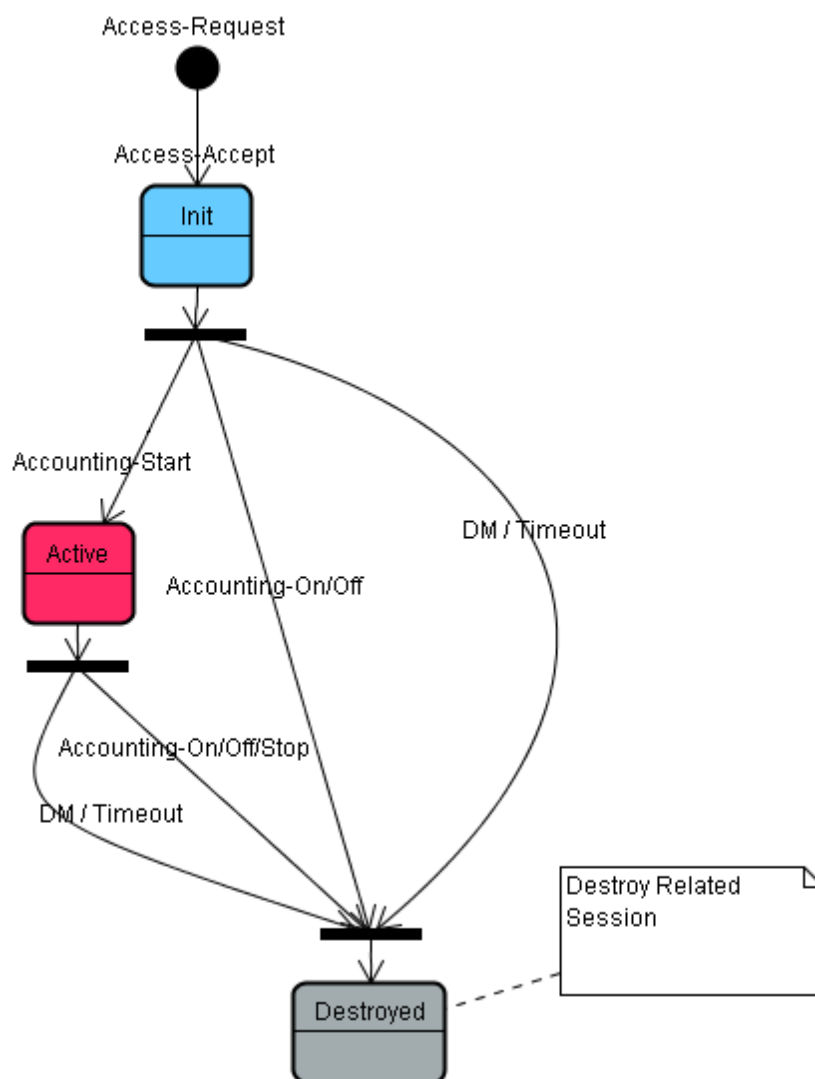


Figure 16 Session State Diagram

The following accounting messages are supported by IPWorks AAA:

- Accounting-Request (Start): This is received at start of service delivery. At this point, the AAA server considers the accounting session as active.
- Accounting-Request (Interim-Update) This can be received at any time during service delivery and is used to update the information related to the accounting session.
- Accounting-Request (Stop): This is received at service completion. At this point, the AAA server considers the accounting session completed, and allocated resources are released.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

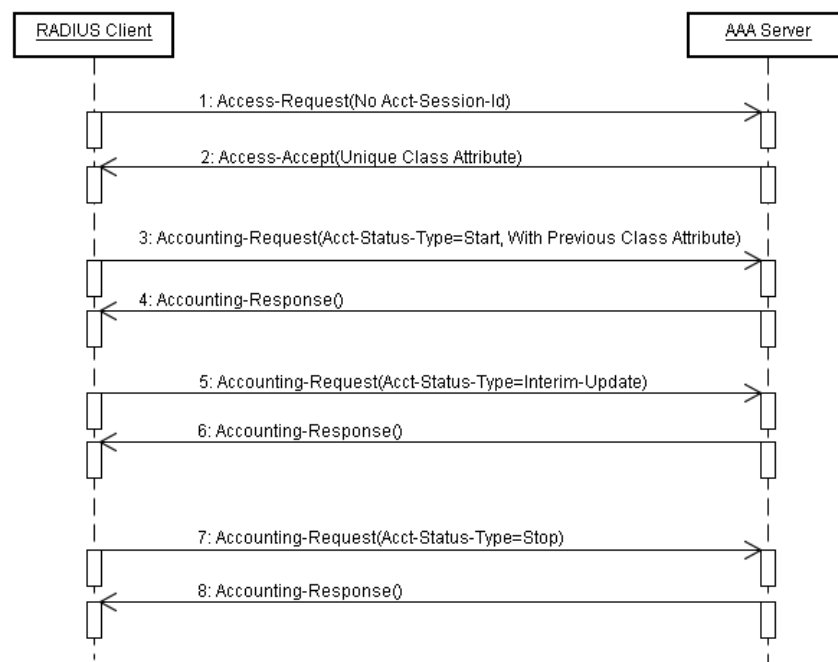
- Accounting-Request (Accounting-On): This notifies the AAA server of a start up condition in the remote NAS. This causes the AAA server to release assigned session resources such as assigned IP address.
- Accounting-Request (Accounting-Off): This notifies the AAA server of a shutdown condition in the remote NAS. This causes AAA Server to release assigned session resources.

Each Accounting-Request message is responded by AAA Server with an Accounting-Response if it has been successfully handled.

3.3.2

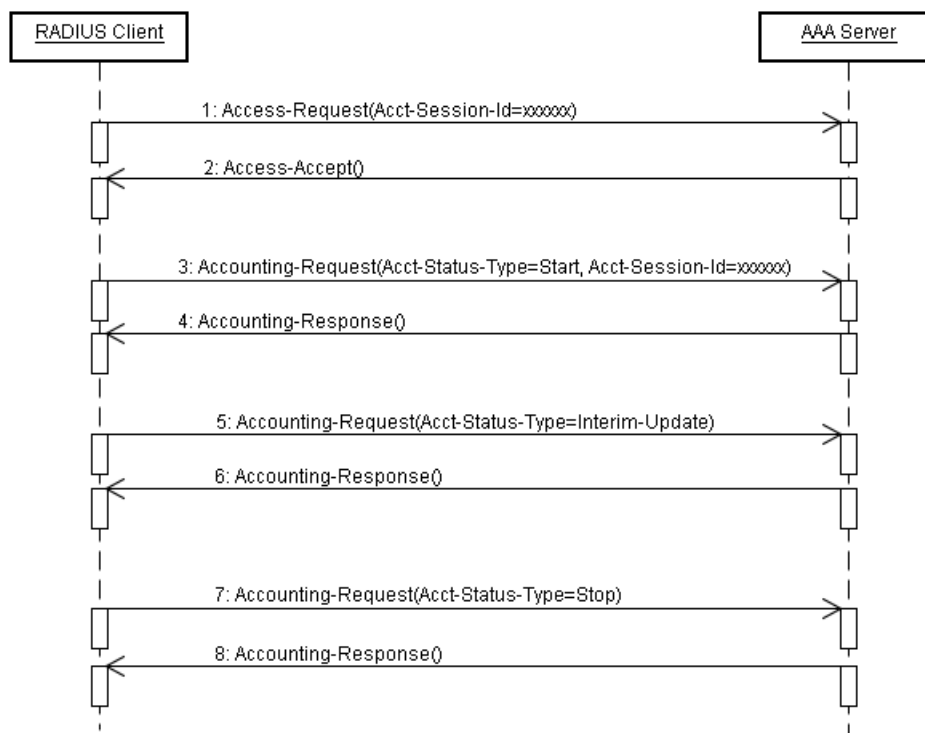
Session Correlation

IPWorks AAA allows using Class or Acct-Session-Id attribute to correlate the session messages (Access-Request and Accounting Request). And the following two sequence diagrams present a brief description of these two scenarios.



Scenario 1 Session Correlation using Class

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference



Scenario 2 Session Correlation using Acct-Session-Id

The IPWorks AAA server assumes the following guidelines to tie Access-Request and Accounting-Request messages:

- If the NAS includes the Acct-Session-Id attribute in the Access-Request message, then it must include the same Acct-Session-Id in subsequent Accounting-Request messages sent to IPWorks AAA. IPWorks AAA also needs an identification attribute for the NAS such as the NAS-Identifier, NAS-IP-Address or NAS-IPv6-Address.
- If the NAS does not include Acct-Session-Id attributes, the AAA Server makes use of the RADIUS Class attribute to tie authentication and accounting sessions.

The AAA server automatically generates a Class attribute (not configurable in the Reply List), which is sent in Access-Accept message as the correlation information from the AAA server back to the RADIUS client. Subsequent Accounting-Request messages sent from the RADIUS client towards AAA server must include this Class attribute, so it can be determined if the session has been previously authorized.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- When the AAA server acts as a proxy, if the Access-Request received does not include Acct-Session-Id and the corresponding Access-Accept sent by the remote server does not include Class attribute, then a Class attribute is automatically generated (not configurable in the Reply List) by the AAA server and added to the Access-Accept before sending it to the client.
- If neither the Acct-Session-Id nor the Class attributes match a previously authorized session, or there is no Class attribute in the accounting message, IPWorks AAA server cannot determine whether the accounting message has to be handled locally or needs to be sent to another server. In this case, the message is discarded.

Note:

If the NAS includes NAS-IP-Address or NAS-Identifier in Access-Request message, the NAS must include the same NAS-IP-Address or NAS-Identifier respectively in subsequent Accounting-Request messages sent to the IPWorks AAA server. In case both attributes are included in the Access-Request message, then the NAS-IP-Address attribute is the preferred one, and it must be included in subsequent Accounting-Request messages sent to IPWorks AAA.

For supporting MPBN authentication and accounting, IPWorks AAA support to use Acct-Multi-Session-Id to correlate multiple accounting records generated by multiple PDP contexts for a user session.

3.3.3 Session Management

IPWorks AAA support session management function with CLI. The administrator can list and clear the specific session(s) by session ID, session status, user name, NAS identifier, session IP address, IP pool which the session IP address is assigned from, session IPv6 prefix. IPv6 prefix Pool which the session IPv6 is assigned from, and the last session update time range. Or list and clear the specific sessions by a filter rule, the rule can be a combination of one or more session information, such as session status, NAS identifier / IP address, user name, IP pool name, IP address, IPv6 prefix name, IPv6 prefix, the last accounting update time.

For abnormal session, IPWorks support automatic and manual handling. If accounting interim update is supported, the session shall be removed from the database after a specific time since the last update time. The typical time shall be 24 hours or more. If accounting interim update is not supported for the user or NAS, the session updated before a specific time can be removed by administrator with CLI commands.

IPWorks AAA supports session HA feature with a cluster solution. The session data shall survive from single point failure of SW and HW.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3.4 Change-of-Authorization

Change-of-Authorization message can be triggered by an operator or some application servers to notify the NAS of the modification of session authorization attributes. CoA can be applied on dynamic service activation for subscribers.

For example, a subscriber has logged in without a service, so a user can later use the CoA message to activate a service for that subscriber. The RADIUS CoA message is useful when a large number of subscribers already logged on and new services need to be activated for them. It could also be used in deactivating a service.

The RADIUS Change-of-Authorization message includes a series of attributes that have to be configured in ECLI. A User can set each attribute in the issuing command or there can be a default attribute configuration for all the CoA messages. They are defined in the MO CoaFormat, refer to Managed Object Model (MOM) **Error! Reference source not found.** for more information. Please note that the AAACoAMessage must contain at least attributes to uniquely identify the NAS (NAS-IP-Address or NAS-Identifier) and the accounting session on the NAS (Acct-Session-Id, Class).

The NAS replies with a CoA-ACK message if the authorization change action has been successfully performed. Otherwise, a CoA-NAK message will be returned and the results will be shown in the IPWorks CLI.

3.5 Session Disconnect

The IPWorks AAA server supports to issue the Disconnect-Request messages to notify a NAS about the termination of the accounting sessions manually or automatically. In generic scenario, the operator can force a session termination using CLI command manually. In WLAN AAA scenario IPWorks AAA can receive notifications from HLR about the user status change and according to the notifications contents to decide whether send Disconnect-Request to terminate the accounting session automatically or not.

The RADIUS Disconnect-Request includes a series of attributes that are almost the same as CoA message. Please refer to the MO DmFormat in Managed Object Model (MOM) **Error! Reference source not found.** for more details.

The NAS responds to the Disconnect-Request message with a Disconnect-ACK message (if all associated session context is discarded and the user session is no longer connected) or a Disconnect-NAK message (if the NAS was unable to disconnect the session and discard all associated session context). In both cases, IPWorks AAA will release the allocated resources.

Once disconnection is performed, the AAA server might receive an Accounting-Request (Stop) message from the NAS.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

The following figure shows an example of the RADIUS message flow between the AAA server and a DAS (NAS or Proxy) when the user session is terminated by means of the Disconnect-Request message:

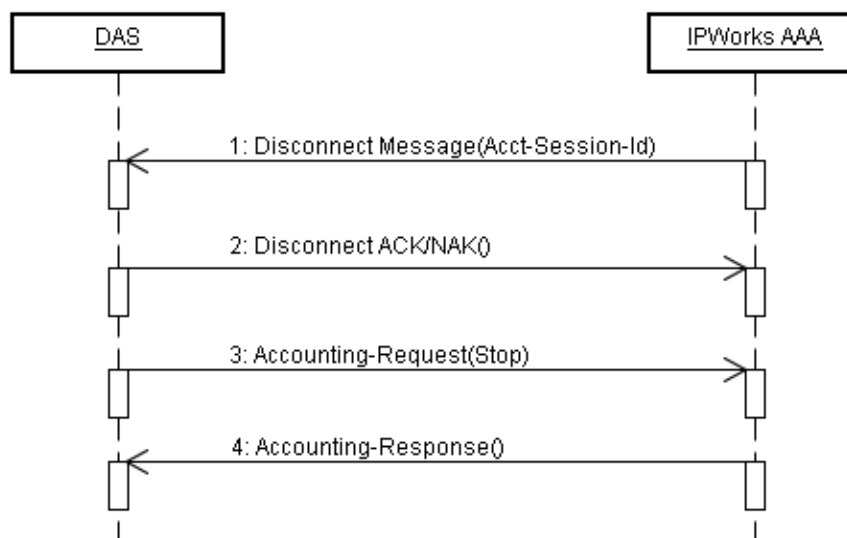


Figure 97 Session Disconnection Scenario

3.6 Proxy Server

The IPWorks Radius AAA server acts as a RADIUS proxy server between a NAS and a Home AAA server as shown in **Error! Reference source not found.18.**

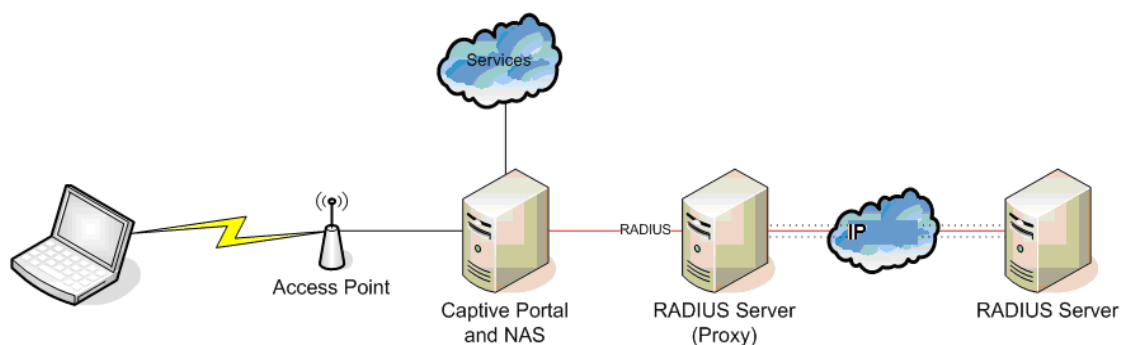


Figure 18 IPWorks AAA as Proxy Server

The following proxy behaviors are supported:

- Forwarding the access/accounting-request message to the remote server and forwarding the response from the remote server to the client.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- Forwarding the DM/CoA message to the NAS (radius client) and forwarding the response from NAS to remote server.

3.6.1 Access/Accounting Message Proxy

3.6.1.1 Proxy Realm Configuration

AAA server forwards the Access/Accounting message to the remote AAA server based on the realm information. All realms, policies and other information needed by proxy functionality are stored in the configuration file or Information Model Management (IMM).

IPWorks AAA can be configured to fetch the realm information from the following specific AVPs according to priority:

- User-Name
- Called-Station-Id
- NAS-Identifier

For example, if an operator configures the parameter "getRealmFrom=User-Name||Called-Station-Id", the AAA server fetches the realm value from the *User-Name* AVP first and check if it exists in the pre-configured realm list firstly:

- If the value of User-Name matches with any realm in the list, AAA server uses the matched realm;
- If the value of User-Name does not match with any realm in the list, the AAA server fetches the realm value from the next AVP "Called-Station-Id".

DN of the attribute "getRealmFrom" is: *ManagedElement=<Node Name>,IpworksFunction=1,IPWorksAAARoot=1,IPWorksRadiusAAARoot=1,RadiusAAAService=1,ProxyControl=1*

Figure 19 shows an example of a generated proxy realm format:

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

```
[REALM]
name=default
striprealm=true
access
{
  destination={192.168.23.9}
  requestchecklist=(( Service-Type = 1 || Service-Type = 2 ))
  replychecklist=(( Service-Type = 1 || Service-Type = 2 ))
  requestchangelist={add:Framed-Protocol="1",delete:Service-Type="2",replace:NAS-Port="8000":'9000'}
  replychangelist=(delete:Service-Type="2")
}

accounting
{
  destination={192.168.23.9}
}

[REALM]
name=/REGEX/^[A-Fa-f0-9]{2,}[5][A-Fa-f0-9]{2}$
striprealm=false
access
{
  destination={10.170.4.30,10.170.4.31,10.170.4.32}
}

accounting
{
  destination=local
}
```

Figure 19 Proxy Realm Format example

3.6.1.2 IPWorks AAA Proxy Functionality

Base on the configured realm information, IPWorks AAA supports to specify different proxy behaviors for different realms:

1. **RealmName:** The RealmName is the identifier of an AAARealm item. RealmName can be either of the following values:

- a realmvalue for exact matching
- a regular expression for format matching

Figure 20 shows the procedure of how AAA server selecting the matched AAARealm item:

Prepared (also subject responsible if other)		No.		
		59/155 17-AVA 901 16 Uen		
Approved	Checked	Date	Rev	Reference
		2018-09-20	C	

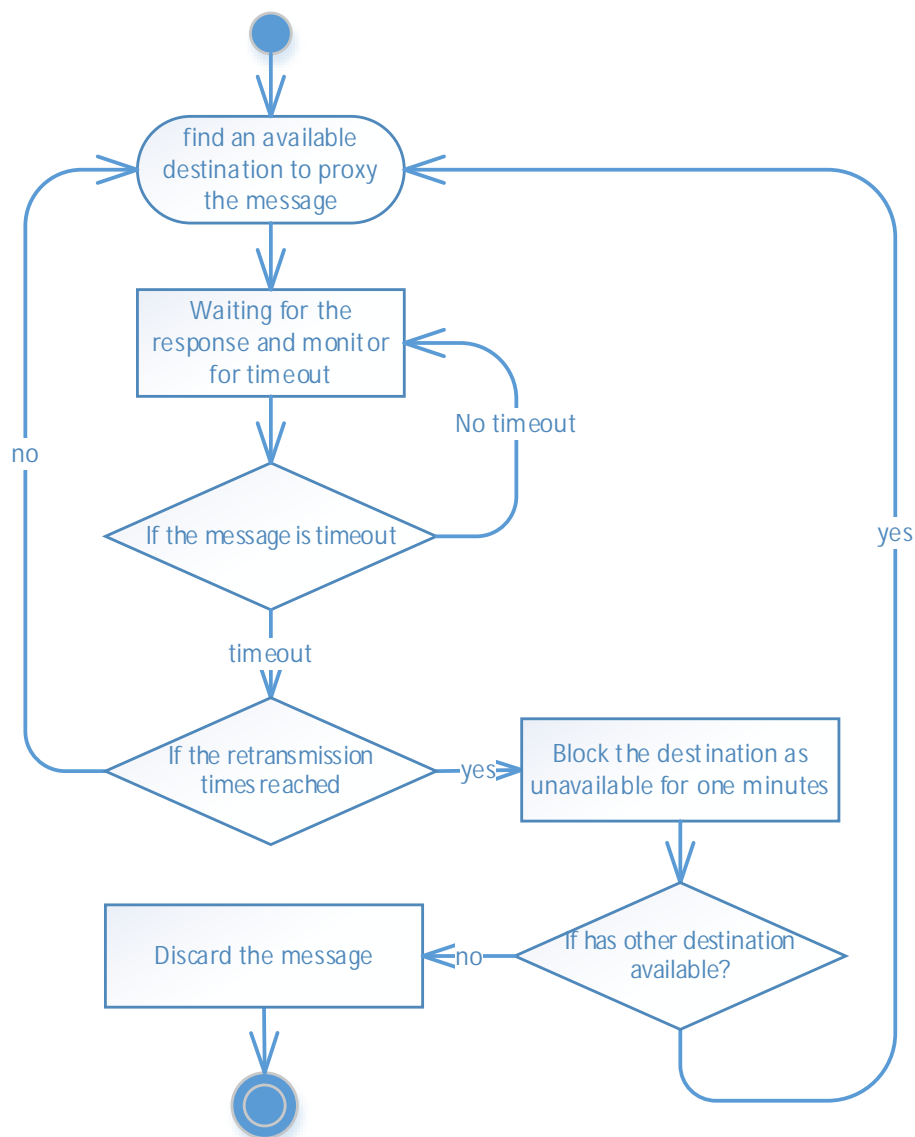


Figure 20 Select matched AAARealm Procedure

2. **StripRealm:** When the realm value is included in *User-Name* AVP, it might display in "*username@realm*" format. Here, StripRealm attribute can be used to specify whether the value of User-Name needs to be changed before AAA server proxies the message to the remote server. If striprealm is set to true, the realm of *User-Name* will be stripped.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3. **Destination Configuration:** IPWork AAA supports the configuration of different destinations for the access and accounting messages independently. The AuthDest and AcctDest value can be set as “local” to specify handling the message in local AAA or remote AAA IP address. The remote AAA IP can be either a single IP address or an IP address list.

Each realm can be configured with several addresses, but each RADIUS message can only be forwarded to one remote address. If multiple destination IP addresses are configured for one realm, the users will follow the configuration order as shown in the following logic:

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2018-09-20	Rev C
		Reference	

Check from **Destination1** to **Destination 2** to **Destination N** until an available address is found.

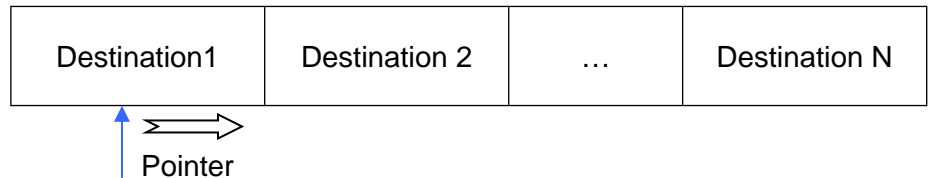


Figure 21 Proxy Destination Address Pool

4. **ProxyRule:** The IPWorks AAA proxy supports the add, removal and modification of the message attributes through the AAAProxyRule configuration which includes the requestchecklist, requestchangelist, replychecklist and replychangelist. The requestchecklist and requestchangelist specify how to check and change the attributes for the **Access Request** message. The replychecklist and replychangelist specify how to check and change the attributes for the **Access Accept** message.

For requestchangelist and replychangelist, the format is like “add:xxx= , delete:xxx=, replace:xxx=old:new” :

- a) **‘add’** means adding an attribute. If an attribute already exists and doesnot allow multiple values, new attribute will not be added.
 - b) **‘delete’** means deleting an attribute with a definite value.
delete:xxx=“*” means no matter what the value of xxx is, the attribute must be deleted.
 - c) **‘replace’** means replacing an the old value of an attributes with a new value. For example, *replace:frame-protocol=“frame:PPP”* means changing the value of frame-protocol from frame to PPP.
5. **Message Modification:** IPWorks AAA supports the modification of the proxy Radius message automatically according to the requirement. IPWorks AAA can replace the NAS related attributes, for example, IP address in the proxy request with its own address and recover it to the original one in the corresponding responses. Some encrypted attributes in the incoming RADIUS message can also be decrypted and re-encrypted using the shared secret of the next RADIUS server.
 6. **Proxy-State:** Proxy-State is handled in the following two ways by IPWorks AAA:

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- a) When the message passes the proxy server, the proxy server appends the Proxy-State to the end of the attributes in the RADIUS message. It strips the added Proxy-State in the response message;
- b) When the message passes the proxy server, the proxy server strips all the Proxy-State in the RADIUS message and then sends the message to the next node, in the response message. The proxy server will then restore all the stripped Proxy-State to the attributes.

DN of the attributes "appendProxyState" is:

ManagedElement=<Node

Name>,IpworksFunction=1,IPWorksAAARoot=1,IPWorksRadiusAAARoot=1,RadiusAAAService=1,ProxyControl=1

3.6.1.3 IPWorks AAA Proxy Type

Depending on different configurations, IPWorks AAA server can work as a standalone AAA server or a proxy AAA server or both standalone and proxy AAA server simultaneously.

Figure 22 shows a detailed procedure of how IPWorks AAA handling the incoming Radius access/accounting message in different proxy types.

Prepared (also subject responsible if other)		No.		
		59/155 17-AVA 901 16 Uen		
Approved	Checked	Date	Rev	Reference
		2018-09-20	C	

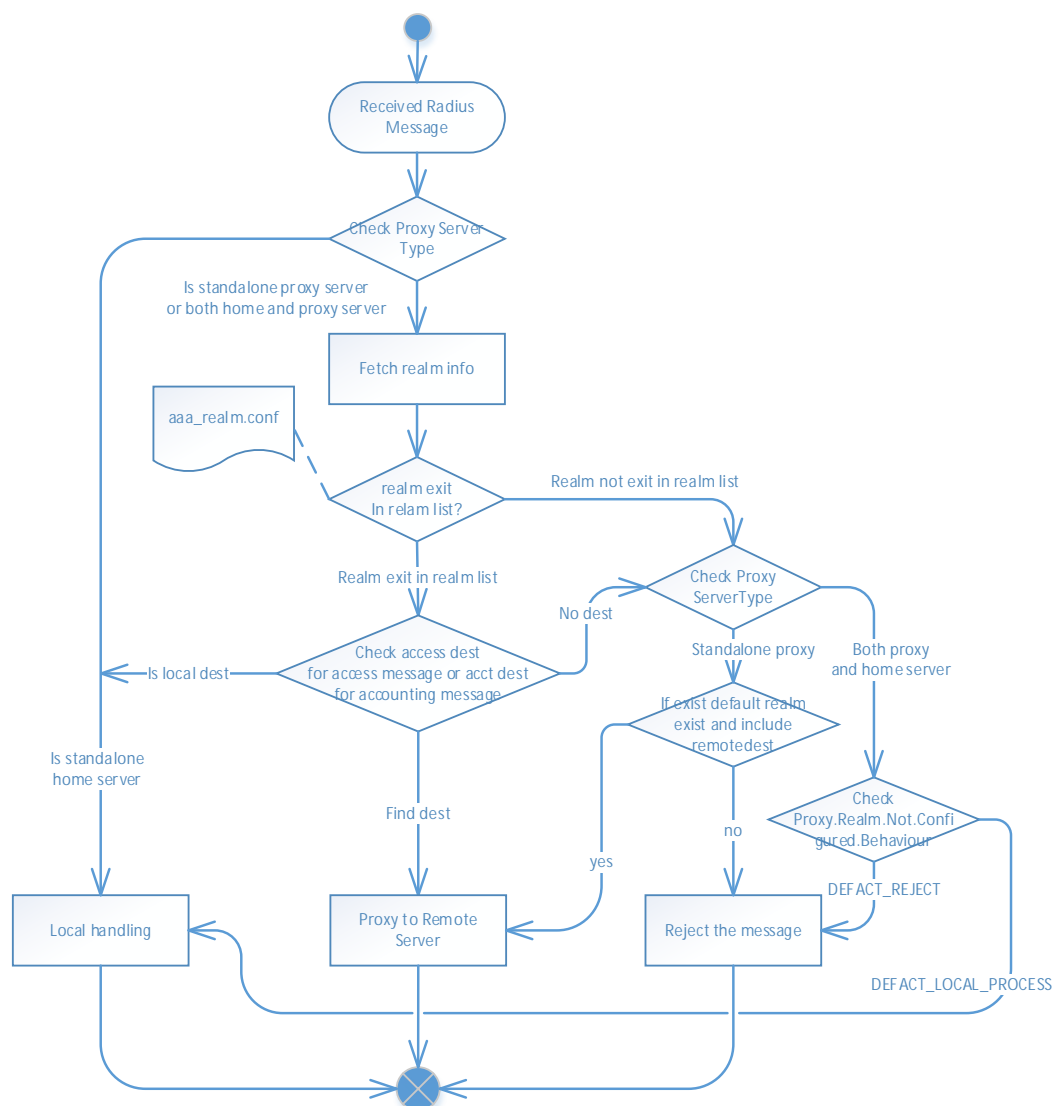


Figure 22 Incoming Message Handling Procedure in Different AAA Proxy Types

Prepared (also subject responsible if other)		No.		
		59/155 17-AVA 901 16 Uen		
Approved	Checked	Date	Rev	Reference
		2018-09-20	C	

3.6.1.4 Message Proxy Retransmission

IPWorks AAA supports the retransmission of the proxy request message if no response message is received within a certain period. There is a thread running in the Proxy module and continuously checking the recorded messages.

For a realm with many destinations, the proxy server sends the message to the destinations one by one in a round-robin algorithm. Each destination has timeout and retransmission limitations that control the transmission. For details on how to configure the limitation parameters.

Figure 23 shows the proxy retransmission procedure:

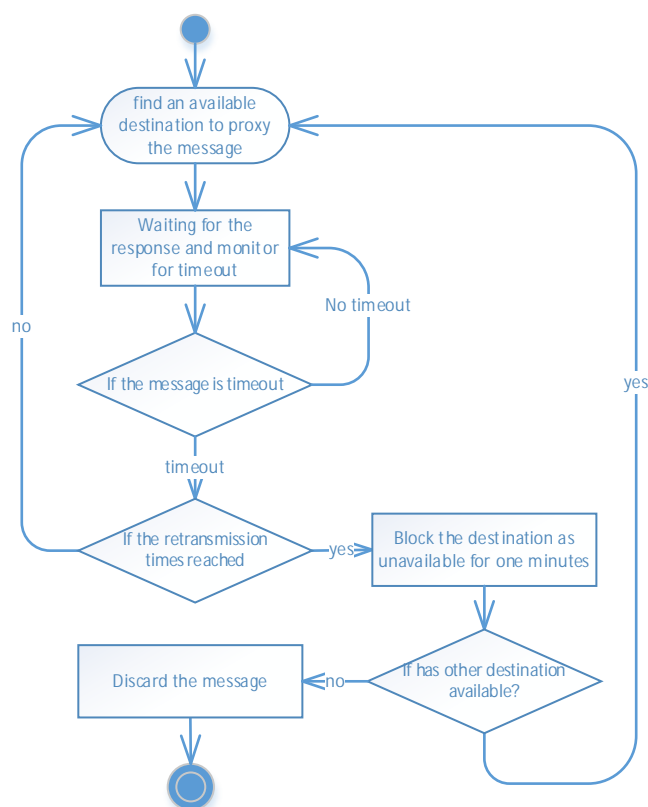


Figure 23 Proxy Retransmission Procedure

3.6.1.5 Access/Accounting Message Proxy Handling Procedure

Figure 24 shows the procedure of AAA Server, as a proxy server, handling the access/accounting message:

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

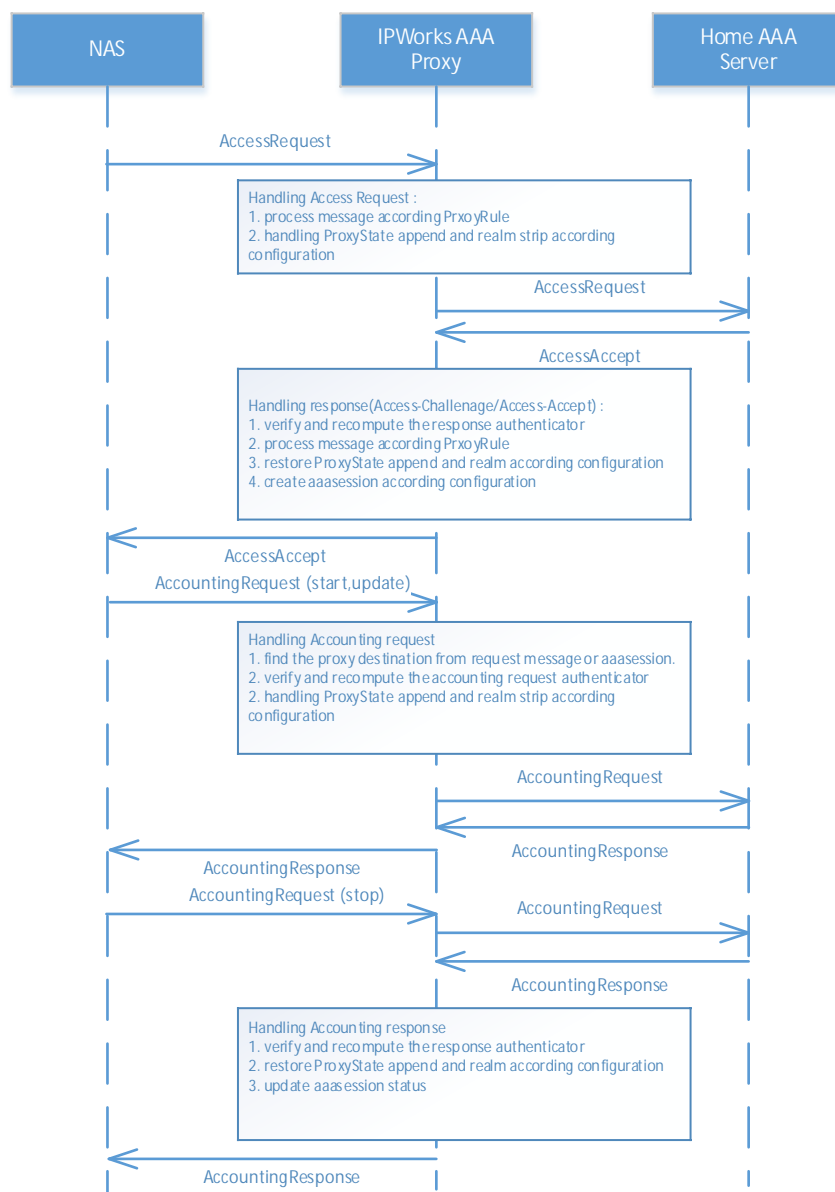


Figure 24 Access/Accounting Message Proxy Handling Procedure

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

Handling Proxy Access Request Message

The following lists the procedure of handling the proxy access response message:

- AAA Server receives a request from a RADIUS client (such as a NAS);
- AAA Server forwards the request to a remote RADIUS server;
- AAA Server receives the response from the remote server;
- AAA Server forwards the response to the client;

Handling Proxy Access Response Message

The following lists the procedure of handling the proxy access response message:

- The proxy server gets the record of its request message based on the internal message ID;
- The proxy server verifies and re-computes the response authenticator in the message;
- For Access-Accept message, apply the Checklist for Access-Accept message;
- For Access-Accept message, add/modify/delete attributes based on local policy and handle "Proxy-State" attribute based on rfc;
- The proxy server gets the IP and port of the client which sent its request before;
- The proxy server restores the stripped realm field;
- The proxy server removes the record of its request message in the core process;

Handling Proxy Accounting Request Message

The following lists the procedure of handling the proxy accounting request message:

- The proxy server forwards the Accounting Request and does not send a reply until it receives the matching reply from the upstream server;
- The proxy server tries to find the proxy destination according to realm field or the related aaasession in the database;

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- The proxy server verifies and re-computes the request authenticator for the accounting request message;
- The proxy server appends/strips the Proxy-State similar to handling the Access request;
- The proxy server stores the forwarded request message data in the core process;

Handling Proxy Accounting Response Message

The following lists the procedure of handling the proxy accounting response message:

- The proxy server gets the record of its request message based on the internal message ID;
- The proxy server verifies and re-computes the accounting response authenticator;
- The proxy server gets the IP and port of the client which sent its request before;
- The proxy server restores the Proxy-State and stripped realm field;
- The proxy server removes the record of its request message in the core process;

3.6.2 DM/COA message Proxy

3.6.2.1 General DM/COA Message Proxy

IPWorks AAA supports to proxy DM/COA-based aaasession information which helps find the original NAS IP address according to the DM/COA message:

1. After Access-Request/Accept and Accounting-Request/Response interchange, the session is set up on the proxy server and the home server. This session records the NAS source IP, the home AAA server IP, the acct-session-id and the class value as shown in the following figure;
2. When the Server Manager on the home Server triggers a CoA/Disconnect message with "Acct-Session-ID"&"Class", the message is sent to the Proxy Server;

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3. When the proxy server gets a CoA/Disconnect-Request with "Acct-Session-ID"&"Class", it uses these two values combined with the home AAA server IP address to search for the related sessions. And then find the original NAS IP address for redirecting messages;

4. After receiving ACK/NAK from NAS, the proxy server forwards the response message to the home server.

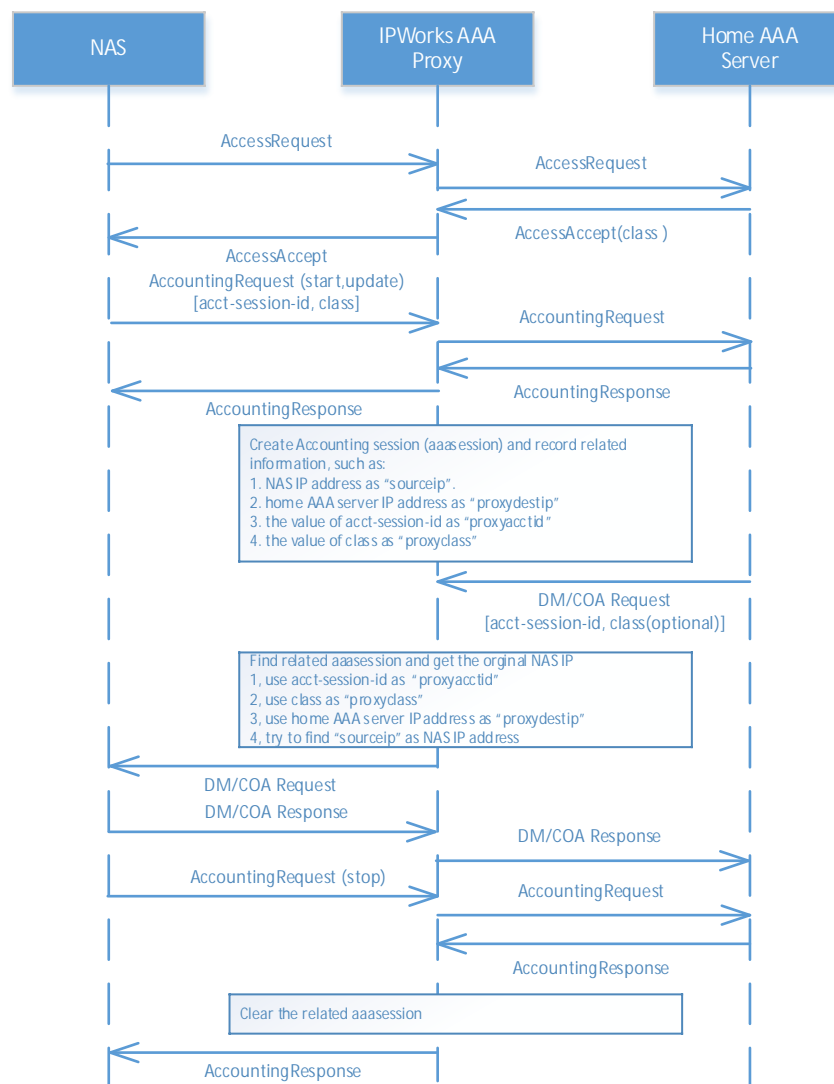


Figure 25 DM/COA Message Proxy Handling Procedure

The proxy functionality for CoA/DM is based on the general proxy functionality and the following handlings are specific for CoA/DM messages:

1. Forwarding the request message to NAS

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

- With the Session manager, based on the identification attributes in the request message, the Core Server can get the destination IP&port and the NAS&Session identification attributes in the forwarded message.
- The attribute “Message-Authenticator” in the forwarded message needs to be calculated if needed.
- AAA server replies with **NAK** to the CoA/Disconnect request message if it cannot find the only destination or has some message error.

2. Replying to messages from NAS

- The proxy server validates the attribute “Message-Authenticator” in the response message from NAS.
- The proxy server Update/add/delete attribute in the ACK/NAK message based on the configuration.

3.6.2.2 DM/COA Message Proxy based on Message

For OpenSSID scenario related to EWG based architecture, IPWorks AAA supports the proxy DM/COA message based on the value of “Acct-Sess-Id”. There is no need to create Proxy aaasession in authentication proxy procedure with this behavior to improve performance and deduce NDB load.

In this scenario, LBO GW adds its IP address as the prefix of the Acct-Sess-Id value, which helps IPWorks AAA fetch the IP address from the DM/COM message. The acct-session-id format is like the following:

- The GGSN or PGW IP address and Charging-ID concatenated in a UTF-8–encoded hexadecimal. The GGSN or PGW IP address used is from the gnS5AddressRange.
- E.g **0A579D42**00AAE620 – 10.87.157.66

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

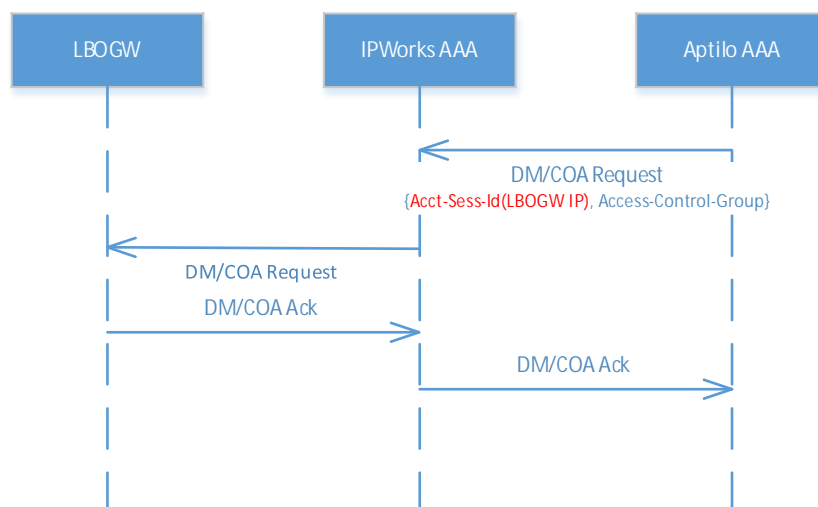


Figure 26 DM/COA Message Proxy based-on Acct-Session-Id

3.7 Overload Protection

If a traffic load exceeds the engineered capacity, IPWorks Radius AAA server starts the AAA Overload Protection mechanism to handle the traffic with some reduced capacity and maintain the established session to avoid snowball effects. Such protection mechanism consists of two parts: Overload Discovery and Overload Control.

3.7.1 Overload Discovery

In IPWorks Radius AAA server, Radius Backend response to monitor the occurred overload.

In Radius Backend, the incoming traffic messages are buffered in message queues. The traffic handling processes monitor the length of the message queue to check the occurred overload. In normal cases, the length of message queue is very short because all messages to be processed are handled by the worker threads.

If the length of message queues exceeds a threshold value (detailed condition can be found in below table), Radius Backend starts the overload control mechanism.

Congestion level	Condition
5	acctCon >= 0.2

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

4	Either one of the condition applies: <ul style="list-style-type: none">acctCon >= 0.05 && normalMsgCon >0.4acctCon >= 0.1
3	acctCon >= 0.05 && normalMsgCon < 0.4
2	normalMsgCon >= 0.4
1	normalMsgCon >= 0.1
0	acctCon < 0.01 && normalMsgCon < 0.01 Note: Congestion Level 0 means no overload happens.

Where:

- acctCon: the usage of the Accounting-Request Queue.
- normalMsgCon: the usage of the Authentication Queue

3.7.2 Overload Control in Radius Backend

When the overload happens, the Radius Backend starts to control the number of worker threads that handle different message queues. The following figure shows the working flow of the Overload Control mechanism.

Prepared (also subject responsible if other)		No.		
		59/155 17-AVA 901 16 Uen		
Approved	Checked	Date	Rev	Reference
		2018-09-20	C	

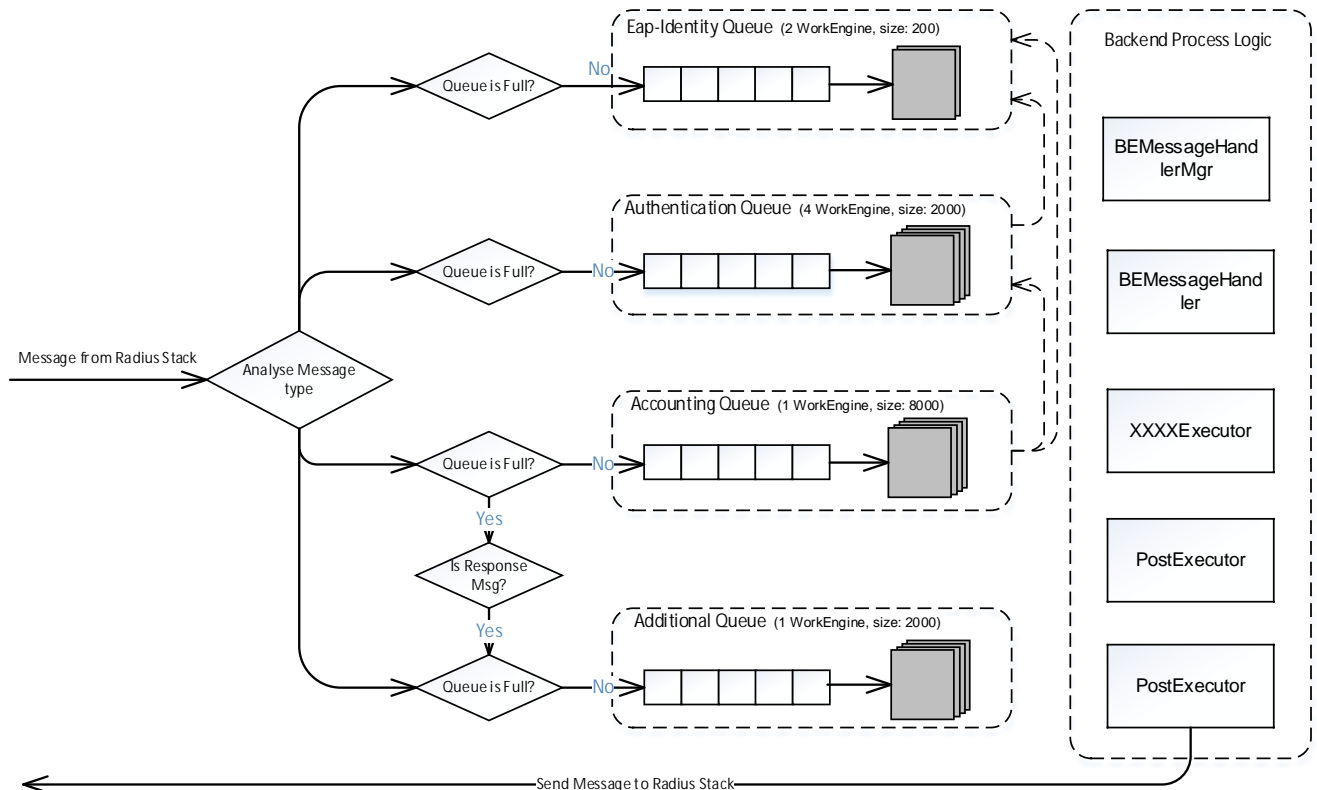


Figure 37 Overload Control Mechanism

Firstly, all received incoming messages are parsed and classified into three different traffic buffer queues:

1. Accounting-Request Queue
2. Authentication Queue
3. Eap-Identity Queue

All the message queues are served by several related worker threads. These threads pick the traffic message from the buffer queue for further handling. If congestion is discovered, Radius Backend adjusts the worker thread number of each message queue to reduce specific message handling capability. Radius AAA will try to handle the messages of the session established (Accounting message) or session establishment is ongoing (Authentication message). Since new session is established slowly, the new message with high priority will also decreased. The adjustment is based on the following rules:

The basic principle of Radius AAA suppresses the handling capability is first to suppress the eap-identity message queue handling, then suppress the authentication message queue handling.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2018-09-20	Rev C
		Reference	

Congestion Level	Isolate Work Engine Number		Description
	EAP_IDENT Queue	Normal_MSG Queue	
5	2	4	Radius Backend blocks all the worker threads for eap-identity queue and all the worker threads for normal message queue (Authentication queue). Thus only accounting messages will be handled with maximum capability.
4	2	3	Radius Backend blocks all the worker threads for eap-identity queue and keeps 1 worker thread for normal message queue (Authentication queue). Thus accounting messages will be handled with maximum capability and part of authentication messages will be handled.
3	1	2	Radius Backend blocks 1 worker thread for eap-identity queue and 2 worker threads for normal message queue (Authentication queue).
2	2	0	Radius Backend blocks all the worker threads for eap-identity queue. Thus accounting message and authentication message will be handled with max capability.
1	1	0	Radius Backend blocks 1 worker thread for eap-identity queue to reduce new session established.
0	0	0	No block.

- For Eap-Identity Request Queue, the Traffic monitor in Radius Backend adjusts the sending rate according to the occurred sending delay times in a specified interval.
- For Accounting-Request Queue and Ongoing Access-Request Queue, the traffic sender always sends the message as fast as possible without controlling the traffic sending rate.
- Ongoing Access-Request Queue is used for multi-round authentication protocols such as EAP. Typically, users continually retry an attempt to gain access, increasing the load even further. IPWorks Radius AAA server preferentially accepts the RADIUS Access-Request packets containing a valid State attribute, so that the multi-round authentication conversations, once begun, is more likely to succeed.

The Radius AAA session already established is maintained with highest priority, so if the length of Accounting-Request Queue exceeds a threshold, the Traffic Coordinator reduces the traffic sending rate for the initial request to ensure the accounting message can be handled with high priority.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

3.7.3 Message Discard under Overload

With traffic control, some traffic messages cannot be put into the corresponding traffic buffer for handling. Radius Backend directly drops the messages.

3.8 Authentication Support for Fixed Access IPoE

3.8.1 RB and BBF VSA

AAA supports all of the following AVPs:

- Redback (Ericsson-AB) Vendor Specific AVPs (VSAs). Vendor ID=2352
- BBF (Broadband Forum) Vendor Specific AVPs(VSAs). Vendor ID=3562.

For more information, refer to **Section Radius-Supported RB and BBF Attributes** in IPWorks AAA Server-AAA Clients Gi Interface, Reference [18].

3.8.2 Fix Access IPoE Authentication

3.8.2.1 Non-Ericsson BNG IPoE Access

For Non-Ericsson Broad Network Gateway (BNG) users, AAA supports the basic PAP or CHAP authentication procedures as described in [Section 3.1 Authentication](#).

3.8.2.2 Ericsson BNG IPoE Access

Figure 38 shows the authentication procedure of Ericsson BNG IPoE Access. When BNG sends an access-request to AAA, AAA uses the Access Loop Identifier configured in IPWorks to check whether anything is matched in the access-request message sent from BNG:

- If AAA finds the PAP password AVP, it authenticates the user with PAP procedure;
- If AAA finds the CHAP password AVP, it authenticates the user with CHAP procedure;
- If AAA finds no password AVP, it authenticates the user with no password procedure.

If AAA fails to authenticate with IPoE user, it falls back to the legacy WIFI CLIPS authentication.

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

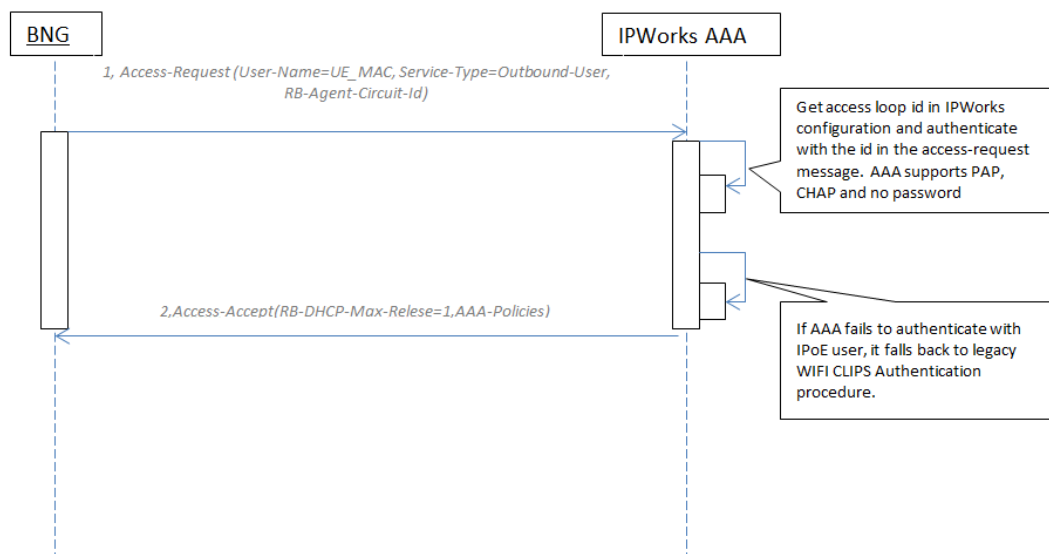


Figure 38 Ericsson BNG IPoE Access Procedure

The difference between Non-Ericsson and Ericsson BNG users is When BNG sends a request to AAA, AAA uses the Access Loop Identifier as the user name for authentication. The Access Loop ID is configurable according to customer's requirement, which can be either of the following:

- NAS-Port-Id
- RB-Agent-Circuit-Id
- RB-Agent-Remote-Id
- BBF-Agent-Circuit-Id
- BBF-Agent-Remote-Id
- Calling-Station-ID

4 Operational Conditions

4.1 Configurable Parameters

-

4.2 Commands and User Procedures

-

4.3 Charging

-

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-20	Rev C	Reference

4.4 Characteristics

-

5 Standard Compliance Statement

See IPWorks Statement of Compliance [11] .

6 Miscellaneous

7 Terminology

7.1 Abbreviations

AAA	Authentication, Authorization, Accounting
APN	Access Point Name
AVP	Attribute Value Pair
CHAP	Challenge-Handshake Authentication Protocol
CoA	Change of Authorization
DAS	Dynamic Authorization Server
DM	Disconnect Message
MSISDN	Mobile Station International ISDN Number
NAS	Network Access Server
PAP	Password Authentication Protocol
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
BNG	Broadband Network Gateway
RB	Redback
BBF	Broadband Forum

7.2 Definitions

-

Prepared (also subject responsible if other)		No. 59/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2018-09-20	Rev C
		Reference	

8

References

- | | | | |
|------|--|-----------------------|-----------|
| [1] | Microsoft Vendor-specific RADIUS Attributes | RFC 2548 | |
| [2] | Remote Authentication Dial In User Service | RFC 2865 | |
| [3] | RADIUS Accounting | RFC 2866 | |
| [4] | RADIUS Accounting Modifications for Tunnel Protocols | RFC 2867 | |
| [5] | RADIUS Attributes for Tunnel Protocol Support | RFC 2868 | |
| [6] | RADIUS Extensions | RFC 2869 | |
| [7] | RADIUS and IPv6 | RFC 3162 | |
| [8] | Dynamic Authorization Extensions to Remote Authentication | RFC 5176 | |
| [9] | Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) | 3GPP TS 29.061 | Release 8 |
| [10] | IWD for IPWorks AAA Server and AAA Client | 22/155 19-CSH 109 085 | |
| [11] | IPWorks Statement of Compliance | 1/174 02-FGC 101 3188 | |
| [12] | Managed Object Model (MOM) | 190 89-LZN 768 0145/2 | |
| [13] | IPWorks Measurement List | 3/006 51-AVA 901 33/2 | |
| [14] | IPWorks Alarm List | 2/006 51-AVA 901 33/2 | |
| [15] | IPWorks Configuration Management | 6/1551-AVA 901 33/2 | |
| [16] | Configure Radius AAA | 49/1543-AVA 901 33/2 | |