

IPWorks AAA Parameter Description

PARAMETER DESCRIPTION

Copyright

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.1.1	Documents	1
1.2	Related Information	1
2	Basic Concept	3
3	Object Format	5
4	Conceptual Overview	7
4.1	AAA	7
4.2	AAA CUDB	9
4.3	AVP	10
5	Managed Objects	21
5.1	AAAIPPool	21
5.2	AAAIPv6PrefixPool	22
5.3	AAAPolicy	24
5.4	AAAProxyRule	27
5.5	AAAREalm	31
5.6	AAAServer	32
5.7	AAASession	32
5.8	AAASubnet	37
5.9	AAAtempIdentityKey	37
5.10	AAAUser	38
5.11	AAANSUser	40
5.12	AAASUserGroup	42
6	Appendix	43
6.1	Example of Configuring 3GPP-User-Location-Info	43
	Reference List	45





1 Introduction

This document describes the AAA objects and fields managed by IPWorks CLI (ipwcli).

Scope

This document covers the following topics:

- Managed Object Model (MOM)
- Managed Object Class Descriptions
- Managed Objects (MO)
- Managed Object Attributes

Target Groups

This document is intended for personnel configuring and fine tuning the IPWorks. It is assumed that readers of this document are familiar with basic concepts and operations of CLI. For details, refer to [Command Line Interface User Guide for IPWorks SS, Reference \[1\]](#).

1.1 Prerequisites

Not Applicable.

1.1.1 Documents

Not Applicable.

1.2 Related Information

Trademark information, typographic conventions, definition and explanation of acronyms and terminology can be found in the following documents:

- Trademark Information
- Glossary of Terms and Acronyms
- Typographic Conventions





2 Basic Concept

This section describes the following:

- The Managed Object Model (MOM) concept
- The Managed Object Class (MOC) concept
- Specific data types
- Specific attributes, for example states
- Conventions

The MOM presents a view of manageable resources in the IPWorks, and attributes and actions associated with the resources.

A Managed Object (MO) is an entity presented to the user for the purpose of controlling the aspects of a function. The object carries attributes that reflect the behavior of the function.

The MOs are identified by means of a naming attribute, also called the Relative Distinguished Name (RDN). The ID part of this attribute is defined when the MO is created, and cannot be changed afterwards. A Local Distinguished Name (LDN) is a sequence of RDNs, which forms a unique name within the node.





3 Object Format

Aliases	The alternative names of an object.
Key	The key is an identifier of an object. The combination of the key field values must be unique for an object.
Required	The required field indicates that the field must be configured, otherwise the CLI generates an error.

— **<Field>**: Field name.

- **Aliases**: The alternative names of a field
- **Type**: Shows whether this field can contain multiple values by putting them into a separated table in the database.
- **Description**: The brief description of a field.





4 Conceptual Overview

This section discusses some of the concepts that are required for managing AAA and AAA objects.

4.1 AAA

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-Authorization (CoA), and Disconnect Messages (DM) to the corresponding target. Proxy servers are commonly used for roaming.

IPWorks AAA supports the session management. A session is related to a series of related radius message exchange, and it is used to record and update the key information according to different radius messages from NAS for user. When authentication or authorization turns to success for a user, a session will be created with status `init`. Accounting-Start message will be used to activate and update the session. The related sessions will be destroyed if the message is Accounting-Stop/On/Off. DM will destroy the related sessions as well. There are two ways to handle the abnormal sessions:

- Automatic removal of abnormal session: If accounting interim update is supported, the abnormal session will be removed from the database after a specific time interval since last update. The typical time interval ranges from 1 hours to 48 hours, default is 24 hours.
- Manual removal of abnormal session: If accounting interim update is not supported for the user or NAS, the abnormal session will never expire and the operator needs to remove it using CLI commands.

AAA server also supports Dynamic Authorization (DA), which allows dynamic changes to a user session. This includes support for disconnecting users and changing authorizations applicable to a user session, which is implemented by disconnect and CoA packets. AAA server sends out CoA and disconnect request messages to NAS and waits for the response from it. So AAA server acts as a Dynamic Authorization Client (DAC) and NAS acts as a Dynamic Authorization Server (DAS).

AAA Server can allocate the IPv4 address, or IPv6 prefix, or both to the user.

Note: "AAA server IPv6 support" function is fully restricted in IPWorks system currently. This function will be supported in future release.

IPv4 address allocation from the IP address pool

Allocate IPv4 address from the IP address pool after successful authentication or authorization. The IP allocation strategy for each user can be adopted in the following ways:

- Allocating static IPv4 address.
- Allocating IPv4 address from a specific pool.
- Allocating IPv4 address according to the Radius client (NAS Identifier, NAS IP Address).
- Allocating IPv4 address according to the Radius client based on APN selection.

The “Framed-IP-Address” attribute in Access-Request message is the hint address that the AAA server must consider in allocating an IP address.

IPv6 address allocation from the IP address pool

Allocate IPv6 prefix from the IP address pool after successful authentication or authorization. The IP allocation strategy for each user can be adopted in the following ways:

- Allocating static IPv6 prefix.
- Allocating IPv6 prefix from a specific pool.
- Allocating IPv6 prefix according to the Radius client (NAS Identifier or NAS IPV6 Address).
- Allocating IPv6 prefix according to the Radius client based on APN selection.

The “Framed-IPv6-Prefix” attribute in Access-Request message is the hint address that the AAA server must consider in allocating an IPv6 prefix.

Figure 1 shows a typical cluster configuration of AAA server. End-user subscribers communicate with an NAS client through the access network. After receiving Radius requests from the NAS clients, the local AAA server handles requests itself, or proxy requests to the remote AAA server. NDB Cluster stores the AAA Server configuration data and user session data. When user detached from the network, CSV files are generated if accounting function is enabled.

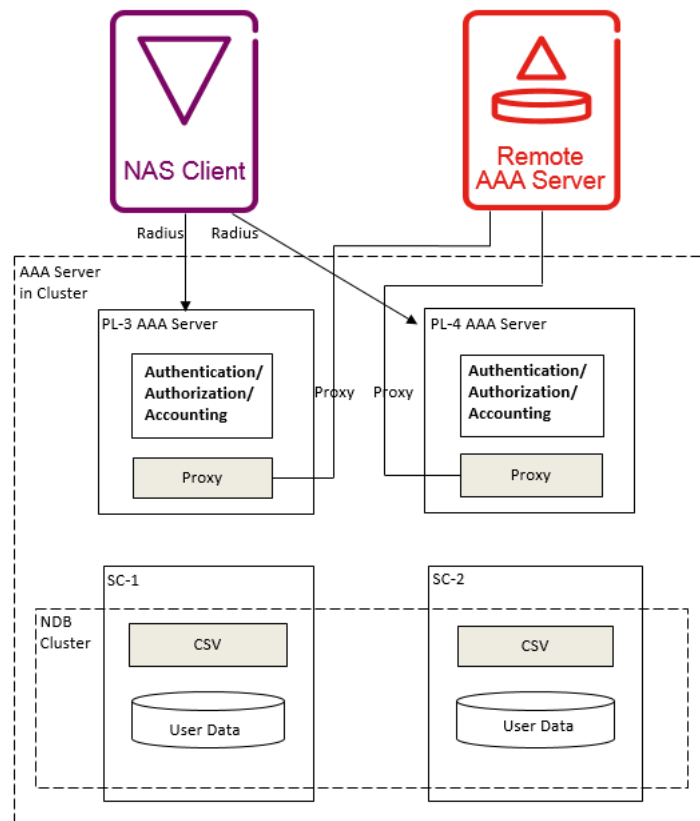


Figure 1 IPWorks AAA Server Cluster

4.2 AAA CUDB

IPWorks supports both monolithic AAA and Data Layered Architecture (DLA) AAA. Monolithic AAA stores user data in the local data node. DLA AAA stores user data in Centralized User Data Base (CUDB).

Figure 2 shows a typical cluster configuration of AAA server when CUDB is configured.

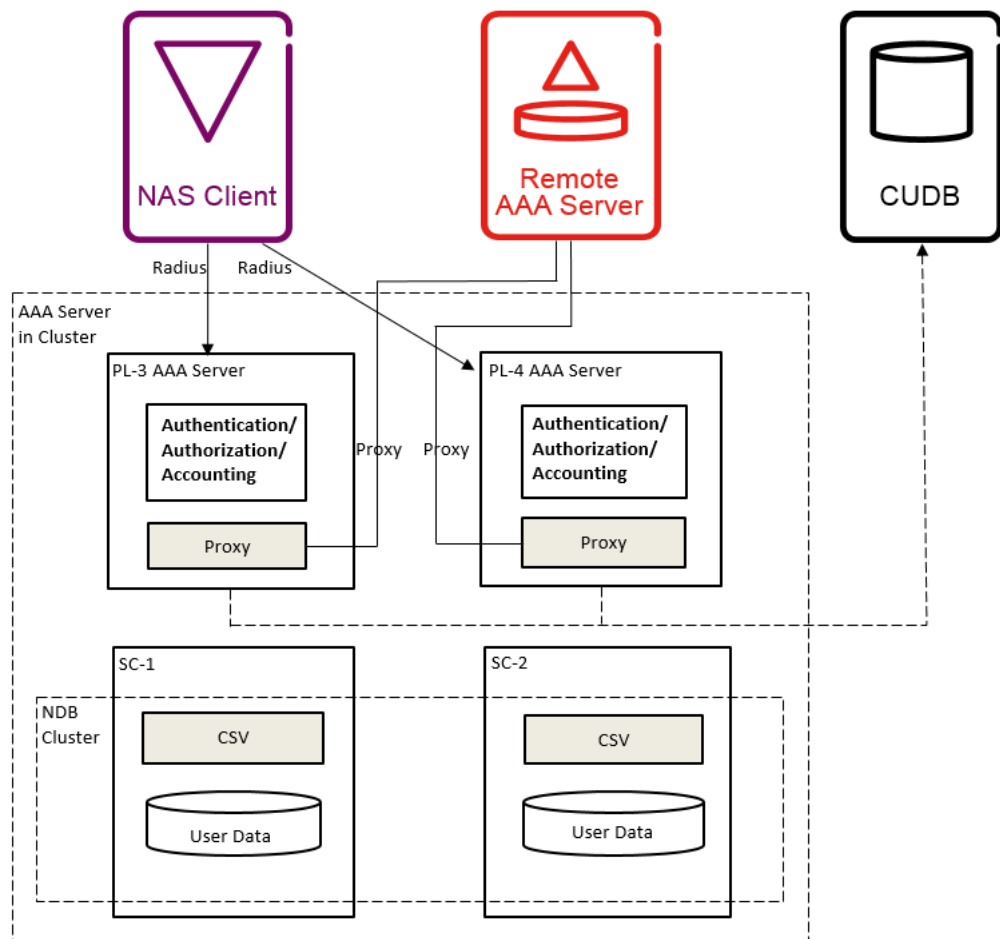


Figure 2 AAA Servers in Cluster with CUDB Configuration

4.3 AVP

Attribute-Value Pair (AVP) is adopted to represent data for IPWorks AAA. Attributes carry the specific authentication, authorization, accounting information and configuration details for the request and reply. Values for specific attributes must comply with the format of those attributes. The following attributes and formats are defined for IPWorks AAA:

Attributes

- Attributes compliant with RFC 2548

See Table 1. For more information on these attributes, refer to Microsoft Vendor-specific RADIUS Attributes, Reference [6].

- Attributes compliant with RFC 2865



- See Table 2. For more information on these attributes, refer to Remote Authentication Dial In User Service (RADIUS), Reference [7].
- Attributes compliant with RFC 2866
 - See Table 3. For more information on these attributes, refer to RADIUS Accounting, Reference [8].
- Attributes compliant with RFC 2867
 - See Table 4. For more information on these attributes, refer to RADIUS Accounting Modifications for Tunnel Protocol Support, Reference [9].
- Attributes compliant with RFC 2868
 - See Table 5. For more information on these attributes, refer to RADIUS Attributes for Tunnel Protocol Support, Reference [10].
- Attributes compliant with RFC 2869
 - See Table 6. For more information on these attributes, refer to RADIUS Extensions, Reference [11].
- Attributes compliant with RFC 3162
 - See Table 7. For more information on these attributes, refer to RADIUS and IPv6, Reference [12].
- Attributes compliant with RFC 4372
 - See Table 8. For more information on these attributes, refer to Chargeable User Identity, Reference [14].
- Attributes compliant with RFC 4675
 - See Table 9. For more information on these attributes, refer to RADIUS Attributes for Virtual LAN and Priority Support, Reference [15].
- Attributes compliant with RFC 4818
 - See Table 10. For more information on these attributes, refer to CRADIUS Delegated-IPv6-Prefix Attribute, Reference [16].
- Attributes compliant with RFC 4849
 - See Table 11. For more information on these attributes, refer to RADIUS Filter Rule Attribute, Reference [17].
- Attributes compliant with RFC 5176
 - See Table 12. For more information on these attributes, refer to Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), Reference [18].



- Attributes Compliant with 3GPP TS 29.061 Version 8.2.0 Release 8

See Table 13. For more information on these attributes, refer to 3GPP TS 29.061 Version 8.2.0 Release 8, Reference [19].

- Vendor-specific Attributes

See Table 14.

- Built-in Attributes

See Table 15.

Formats

- String
- Integer
- Enumeration

A set of unsigned integers. The exact listing of all the unsigned integers and their definitions is described in the corresponding RFCs. For example, attribute “Service-Type” has the following enumeration:

- 1: Login
- 2: Framed
- 3: Callback Login
- 4: Callback Framed
- 5: Outbound
- 6: Administrative
- 7: NAS Prompt
- 8: Authenticate Only
- 9: Callback NAS Prompt
- 10: Call Check
- 11: Callback Administrative
- 17: Authorize Only

- IPv4

IPv4 address with the format of <Decimal>.<Decimal>.<Decimal>.<Decimal>. For example, 10.170.4.10.

- IPv6

IPv6 address with the format of <hexadecimal>:<hexadecimal>:<hexadecimal>:<hexadecimal>:<hexadecimal>:<hexadecimal>:<hexadecimal>:<hexadecimal>. For example, CDCD:910A:2222:5498:8475:1111:3900:2020.

- Special Formats

See the following tables for details.



Note: The formats described above and in the following tables are the input formats for CLI.

Table 1 Attributes Compliant with RFC 2548

Attribute	Format	Comment
MS-MPPE-Send-Key	String	
MS-MPPE-Recv-Key	String	
MS-Primary-DNS-Server	IPv4	
MS-Secondary-DNS-Server	IPv4	
MS-Primary-NBNS-Server	IPv4	
MS-Secondary-NBNS-Server	IPv4	

Table 2 Attributes Compliant with RFC 2865

Attribute	Format	Comment
User-Name	String	
User-Password	String	
CHAP-Password	String	
NAS-IP-Address	IPv4	
NAS-Port	Integer	
Service-Type	Enumeration	For special setting about Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), refer to Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), Reference [18]. The value for "Authorize Only" is 17.
Framed-Protocol	Enumeration	
Framed-IP-Address	IPv4	
Framed-IP-Netmask	IPv4	
Framed-Routing	Enumeration	
Filter-Id	String	
Framed-MTU	Integer	
Framed-Compression	Enumeration	
Login-IP-Host	IPv4	
Login-Service	Enumeration	
Login-TCP-Port	Integer	
Reply-Message	String	
Callback-Number	String	
Callback-Id	String	
Framed-Route	String	
Framed-IPX-Network	Integer	



Attribute	Format	Comment
State	String	For the special setting about Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), refer to Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), Reference [18].
Class	String	
Vendor-Specific	String	
Session-Timeout	Integer	Time
Idle-Timeout	Integer	Time
Termination-Action	Enumeration	
Called-Station-Id	String	
Calling-Station-Id	String	
NAS-Identifier	String	
Proxy-State	String	For the special setting about Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), refer to Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), Reference [18].
Login-LAT-Service	String	
Login-LAT-Node	String	
Login-LAT-Group	String	
Framed-AppleTalk-Link	Integer	
Framed-AppleTalk-Network	Integer	
Framed-AppleTalk-Zone	String	
CHAP-Challenge	String	
NAS-Port-Type	Enumeration	
Port-Limit	Integer	
Login-LAT-Port	String	

Table 3 Attributes Compliant with RFC 2866

Attribute	Format	Comment
Acct-Status-Type	Enumeration	
Acct-Delay-Time	Integer	Time
Acct-Input-Octets	Integer	
Acct-Output-Octets	Integer	
Acct-Session-Id	String	
Acct-Authentic	Enumeration	
Acct-Session-Time	Integer	Time
Acct-Input-Packets	Integer	



Attribute	Format	Comment
Acct-Output-Packets	Integer	
Acct-Terminate-Cause	Enumeration	
Acct-Multi-Session-Id	String	
Acct-Link-Count	Integer	

Table 4 Attributes Compliant with RFC 2867

Attribute	Format	Comment
Acct-Tunnel-Connection	String	
Acct-Tunnel-Packets-Lost	Integer	

Table 5 Attributes Compliant with RFC 2868

Attribute	Format	Comment
Tunnel-Type	Integer	
Tunnel-Medium-Type	Integer	
Tunnel-Client-Endpoint	'tag string'	tag is decimal ASCII. For example, Tunnel-Client-Endpoint='01 aaa.test'.
Tunnel-Server-Endpoint	'tag string'	tag is decimal ASCII. For example, Tunnel-Server-Endpoint='01 DDDD'.
Tunnel-Password	'tag salt salt string'	tag and salt are decimal ASCII. string is the unencrypted password. For example, Tunnel-Password='01 11 12 023456abcdef1234123456abcdef1234'.
Tunnel-Private-Group-ID	'tag string'	tag is decimal ASCII. For example, Tunnel-Private-Group-ID='01 AAAA'.
Tunnel-Assignment-ID	'tag string'	tag is decimal ASCII. For example, Tunnel-Assignment-ID='01 1234asd'.
Tunnel-Preference	Integer	
Tunnel-Client-Auth-ID	'tag string'	tag is decimal ASCII. For example, Tunnel-Client-Auth-ID='01 BBBB'.
Tunnel-Server-Auth-ID	'tag string'	tag is decimal ASCII. For example, Tunnel-Server-Auth-ID='01 CCCC'.

Table 6 Attributes Compliant with RFC 2869

Attribute	Format	Comment
Acct-Input-Gigawords	Integer	



Attribute	Format	Comment
Acct-Output-Gigawords	Integer	
Event-Timestamp	Integer	
ARAP-Password	'val1 val2 val3 val4'	val is integer. For example, ARAP-Password= '11 12 13 14'.
ARAP-Features	'val1 val2 val3 val4 val5'	val is integer. For example, ARAP-Features= '11 12 13 14 15'.
ARAP-Zone-Access	Integer	
ARAP-Security	Integer	
ARAP-Security-Data	String	
Password-Retry	Integer	
Prompt	Integer	
Connect-Info	String	
Configuration-Token	String	
EAP-Message	String	
Message-Authenticator	String	For special setting about Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), refer to Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), Reference [18].
ARAP-Challenge-Response	String	
Acct-Interim-Interval	Integer	
NAS-Port-Id	String	
Framed-Pool	String	

Table 7 Attributes Compliant with RFC 3162

Attribute	Format	Comment
NAS-IPv6-Address	IPv6	
Framed-Interface-Id	String	
Framed-IPv6-Prefix	IPv6	
Login-IPv6-Host	IPv6	
Framed-IPv6-Route	String	
Framed-IPv6-Pool	String	



Table 8 Attributes Compliant with RFC 4372

Attribute	Format	Comment
Chargeable-User-Identity	String	A switch to control the reply of Chargeable-User-Identity (CUI) in Access-Accept is available. For detailed information, refer to the section CUI Switch in <i>Configure Radius AAA</i> , Reference [5]

Table 9 Attributes Compliant with RFC 4675

Attribute	Format	Comment
Egress-VLANID	Integer	
Ingress-Filters	Integer	
Egress-VLAN-Name	String	
User-Priority-Table	String	

Table 10 Attributes Compliant with RFC 4818

Attribute	Format	Comment
Delegated-IPv6-Prefix	IPv6	

Table 11 Attributes Compliant with RFC 4849

Attribute	Format	Comment
NAS-Filter-Rule	String	

Table 12 Attributes Compliant with RFC 5176

Attribute	Format	Comment
Error-Cause	Integer	

Table 13 Attributes Compliant with 3GPP TS 29.061 Version 8.2.0 Release 8

Attribute	Format	Comment
3GPP-Allocate-IP-Type	Integer	
3GPP-IMSI	String	
3GPP-Charging-ID	Integer	
3GPP-PDP-Type	Integer	
3GPP-CG-Address	IPv4	
3GPP-GPRS-Negotiated-QoS-Profile	String	
3GPP-SGSN-Address	IPv4	
3GPP-GGSN-Address	IPv4	
3GPP-IMSI-MCC-MNC	String	
3GPP-GGSN-MCC-MNC	String	
3GPP-NSAPI	String	



Attribute	Format	Comment
3GPP-Session-Stop-Indicator	Bit String	The value is 11111111.
3GPP-Selection-Mode	String	
3GPP-Charging-Characteristics	String	
3GPP-CG-IPv6-Address	IPv6	
3GPP-SGSN-IPv6-Address	IPv6	
3GPP-GGSN-IPv6-Address	IPv6	
3GPP-IPv6-DNS-Servers	'ipv6 ipv6 ipv6'	A list of IPv6 addresses. For example, 3GPP-IPv6-DNS-Servers=CD:CD:910A:2222:5498:8475:1111:3900:2020.
3GPP-SGSN-MCC-MNC	String	
3GPP-Tear-down-Indicator	Octet string	0 or 1
3GPP-IMEISV	String	
3GPP-RAT-Type	type	decimal ASCII For example, 3GPP-RAT-Type=101.
3GPP-User-Location-Info	String(dec dec dec ...)	For an example on how to configure it in IPWorks, see Section 6.1 on page 43
3GPP-MS-TimeZone	'timezone daylightSavingTime'	decimal ASCII For example, 3GPP-MS-TimeZone='56 50'.
3GPP-CAMEL-Charging-Info	'dec dec dec dec ...'	decimal ASCII For example, 3GPP-CAMEL-Charging-Info=123.
3GPP-Packet-Filter	N/A	
3GPP-Negotiated-DSCP	code	decimal ASCII For example, 3GPP-Negotiated-DSCP=100.

Table 14 Vendor-specific Attributes

Attribute	Format	Comment
ERICSSON-Prim-Rule-Space-Name	String	
ERICSSON-Sec-Rule-Space-Name	String	
ERICSSON-ACG-ID	String	
ERICSSON-Authorization-Code	'dec dec dec dec'	decimal ASCII For example, ERICSSON-Authorization-Code='81 82 83 84'.
Offload_Indication	String	
GTP-Tunnel-Data	String	

**Note:**

- IPWorks AAA supports dynamic AVP configuration to allow users add any vendor-specific AVP according their requirement.
- In the directory `/etc/ipworks/aaa/dict`, users can configure the `dict-customized.xml` file. The `dict-customized.xml` file shows the format of the vendor-specific AVPs and users can use `perl dict-customized-verify.pl verify_logic dict-customized.xml` to verify the format.

Table 15 Built-in Attributes

Attribute	Format	Comment
System-Time	Integer	The format of System-Time follows the time specification as per section 3.3 in Internet Message Format, Reference [20].
Arrive-Time	N/A	For sequence CSV record
Acct-Start-Time	N/A	For session CSV record
Acct-End-Time	N/A	For session CSV record





5 Managed Objects

This section describes the AAA objects and fields.

5.1 AAAIPPool

A pool stores some IP addresses for AAA server.

Key	Name
Required	Name, Subnet, AddressRange
— Name	
<ul style="list-style-type: none"> • Type: Single • Description: The name of this lease pool (must be unique). 	
— Subnet	
<ul style="list-style-type: none"> • Type: Single • Description: The name of the AAASubnet that contains this lease pool. This subnet should be present. 	
— AddressRange	
<ul style="list-style-type: none"> • Aliases: Range • Description: The range of addresses in the lease pool. The value of this field should be a valid range specification (typically 2 addresses separated by a hyphen). It can also be specified using the standard subnet "slash" notation for example, 10.2.0.0/16. 	
— ClientIP	
<ul style="list-style-type: none"> • Type: Single • Description: The IP address of the Radius client which the pools should be associated with. The Radius client includes "NAS-IP-Address" attribute or "NAS-IPv6-Prefix" attribute in the Radius access request message. 	
— ClientIdentifier	
<ul style="list-style-type: none"> • Type: Single • Description: The identifier of the Radius client which the pools should be associated with. The identifier of the Radius client which sends the Access-Request, will be set in the attribute "NAS-Identifier" of the request. 	



Note: **ClientIP** and **ClientIdentifier** are alternatives, one of them or both can be configured. The **ClientIP** will be preferred when configuring both **ClientIP** and **ClientIdentifier**.

— **ClientAPN**

- **Type:** Single
- **Description:** The APN of the Radius client which the pool is associated with. The APN of the Radius client which sends the Access-Request, will be set in the attribute "Called-Station-Id" of the request.

When the pool is associated with Radius client based on APN selection, the **ClientAPN** must be configured with either **ClientIP** or **ClientIdentifier**, or both. The **ClientIP** based on APN selection will be preferred when configuring both **ClientIP** and **ClientIdentifier** with **ClientAPN**.

— **Realm**

- **Type:** Single
- **Description:** IP address zone, optional field, but if CLF is involved, this field needs to be set.

— **Nextfreeip**

- **Type:** Single
- **Description:** The next free IP in this pool, it is not configurable field but only created and maintained by AAA server.

— **Leasecount**

- **Type:** Single
- **Description:** The lease count of this pool, it is not configurable field but only created and maintained by AAA server.

— **Totalcount**

- **Type:** Single
- **Description:** The count of total IP addresses in this pool, it is not configurable field but only created and maintained by AAA server.

5.2 AAAIPv6PrefixPool

A pool stores some IPv6 prefix addresses for AAA server.

Key	Name
Required	Name, PrefixRange



— **Name**

- **Type:** Single
- **Description:** The name of this IPv6 prefix lease pool policy (must be unique).

— **PrefixLength**

- **Type:** Single
- **Description:** The length of the IPv6 prefix. This is a value between 1 and 64 indicating the IPv6 prefix length in the pool.

— **PrefixRange**

- **Type:** Range
- **Description:** The range of the IPv6 prefix in the lease pool.

Format:

<IPv6 ADDRESS1>/<length1> - <IPv6 ADDRESS2>/<length2>
or <IPv6 ADDRESS>/<length1> - <length2>.

For example:

2012:ABCD:170::/64-2012:ABCD:170:FFFF::/64

or

2012:ABCD:170::/48-64

— **ClientIP**

- **Type:** Single
- **Description:** The IP address of the Radius client which the pools can be associated with. The Radius client includes “NAS-IP-Address” attribute or “NAS-IPv6-Prefix” attribute in the Radius access message.

— **ClientIdentifier**

- **Type:** Single
- **Description:** The identifier of the Radius client which the pools should be associated with. The identifier of the Radius client which sends the Access-Request, will be set in the attribute “NAS-Identifier” of the request.

Note: **ClientIP** and **ClientIdentifier** are alternatives, one of them or both can be configured. The **ClientIP** will be preferred when configuring both **ClientIP** and **ClientIdentifier**.

— **ClientAPN**

- **Type:** Single



- **Description:** The APN of the Radius client which the pools should be associated with. The APN of the Radius client which sends the Access-Request, will be set in the attribute "Called-Station-Id" of the request.

When the pool is associated with Radius client based on APN selection, the ClientAPN must be configured with either **ClientIP** or **ClientIdentifier**, or both. The **ClientIP** based on APN selection will be preferred when configuring both **ClientIP** and **ClientIdentifier** with **ClientAPN**.

— Realm

- **Type:** Single
- **Description:** IP address zone, optional field, but if CLF is involved, this field needs to be set.

— Nextfreeipv6prefix

- **Type:** Single
- **Description:** The next free IPv6 Prefix in this pool, it is not configurable field but only created and maintained by AAA server.

— Leasecount

- **Type:** Single
- **Description:** The lease count of this pool, it is not configurable field but only created and maintained by AAA server.

— Totalcount

- **Type:** Single
- **Description:** The count of total IPv6 prefixes in this pool, it is not configurable field but only created and maintained by AAA server.

5.3 AAAPolicy

The policy is a rule based authorization for AAA Server. It is used for authorization. When an Access-Request message comes, if it matches the policy check rule, it will be treated as a successful authorization, otherwise it will fail. If it is a successful authorization, the policy reply rule will be added to the Access-Accept message.

Note: The performance of authorization will drop if one user is linked to a large number of policies. It is recommended that policies linked directly or indirectly to each user be less than 10.

Aliases AAAPolicy

Key Name

**Required****Name**— **Name**

- **Type:** Single
- **Description:** The name of the policy.

— **Checklist**

- **Type:** Single
- **Description:** The checklist is a check rule of the policy. It is used to check whether the coming AVPs are matched with this check rule. All the AVP names should conform to the AVP name in RFC, except the build-in AVPs such as System-Time.

Syntax:

```
expression := condition | '(' expression ')' | expression
logicalop expression
condition := avpname relop value
logicalop := '&' | '|' | '&&' | '||'
relop := '=' | '==' | '!=' | '>' | '>=' | '<' | '<=' | '?'
```

Where:

- avpname: The attribute. It can be one of the following:

User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-Routing, Filter-Id, Framed-MTU, Framed-Compression, Login-IP-Host, Login-Service, Login-TCP-Port, Reply-Message, Callback-Number, Callback-Id, Framed-Route, Framed-IPX-Network, State, Class, Session-Timeout, Idle-Timeout, Termination-Action, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Framed-AppleTalk-Link, Framed-AppleTalk-Network, Framed-AppleTalk-Zone, Port-Limit, Login-LAT-Port, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Server-Endpoint, Tunnel-Password, Tunnel-Preference, Tunnel-Client-Endpoint, Tunnel-Private-Group-ID, Tunnel-Client-Auth-ID, Tunnel-Server-Auth-ID, Tunnel-Assignment-ID, 3GPP-IPv6-DNS-Servers, 3GPP-Charging-Characteristics, MS-primary-DNS-server, MS-Secondary-DNS-Server, MS-Primary-NBNS-Server, MS-Secondary-NBNS-Server, Framed-IPv6-Prefix, Framed-IPv6-Pool, Framed-Pool, Called-Station-Id, Suggested-Rule-Space, Access-control-group, 3GPP-SGSN-MCC-MNC, Login-IPv6-Host, Framed-IPv6-Route, Framed-Interface-Id, SN-Rad-APN-Name, SN1-Rad-APN-Name, or HW-VPN-Name.

- relop: The relational operator.
- logicalop: The logical operator.



— value: A fixed value or \$SESSION.

For example: Checklist="System-Time >= "10:00 +0800" &&
System-Time <= "20:00 +0800" && (User-Name = "AAATest" &&
(Service-Type = "Framed" || Service-Type = "1"))"

— Replylist

- **Type:** Single
- **Description:** The reply list is a reply rule of the policy. If the Access-Request message is authorized successfully, the reply rule will be added to the Access-Accept message.

Syntax:

```
expression := condition | ', ' expression  
condition := avpname = value  
value := fixed value | $REQUEST
```

Where:

— avpname: The attribute. It can be one of the following:

User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-Routing, Filter-Id, Framed-MTU, Framed-Compression, Login-IP-Host, Login-Service, Login-TCP-Port, Reply-Message, Callback-Number, Callback-Id, Framed-Route, Framed-IPX-Network, State, Class, Session-Timeout, Idle-Timeout, Termination-Action, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Framed-AppleTalk-Link, Framed-AppleTalk-Network, Framed-AppleTalk-Zone, Port-Limit, Login-LAT-Port, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Server-Endpoint, Tunnel-Password, Tunnel-Preference, Tunnel-Client-Endpoint, Tunnel-Private-Group-ID, Tunnel-Client-Auth-ID, Tunnel-Server-Auth-ID, Tunnel-Assignment-ID, 3GPP-IPv6-DNS-Servers, 3GPP-Charging-Characteristics, MS-primary-DNS-server, MS-Secondary-DNS-Server, MS-Primary-NBNS-Server, MS-Secondary-NBNS-Server, Framed-IPv6-Prefix, Framed-IPv6-Pool, Framed-Pool, Called-Station-Id, Suggested-Rule-Space, Access-control-group, 3GPP-SGSN-MCC-MNC, Login-IPv6-Host, Framed-IPv6-Route, or Framed-Interface-Id.

— avpname: The attribute. It can be one of the following:

User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-Routing, Filter-Id, Framed-MTU, Framed-Compression, Login-IP-Host, Login-Service, Login-TCP-Port, Reply-Message, Callback-Number, Callback-Id, Framed-Route, Framed-IPX-Network, State, Class, Session-Timeout, Idle-Timeout, Termination-Action, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Framed-AppleTalk-Link,



Framed-AppleTalk-Network, Framed-AppleTalk-Zone, Port-Limit, Login-LAT-Port, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Server-Endpoint, Tunnel-Password, Tunnel-Preference, Tunnel-Client-Endpoint, Tunnel-Private-Group-ID, Tunnel-Client-Auth-ID, Tunnel-Server-Auth-ID, Tunnel-Assignment-ID, 3GPP-IPv6-DNS-Servers, 3GPP-Charging-Characteristics, MS-primary-DNS-server, MS-Secondary-DNS-Server, MS-Primary-NBNS-Server, MS-Secondary-NBNS-Server, Framed-IPv6-Prefix, Framed-IPv6-Pool, Framed-Pool, Called-Station-Id, Suggested-Rule-Space, Access-control-group, 3GPP-SGSN-MCC-MNC, Login-IPv6-Host, Framed-IPv6-Route, Framed-Interface-Id, SN-Rad-APN-Name, SN1-Rad-APN-Name, or HW-VPN-Name.

— value: It can be a fixed value or \$REQUEST.

For example: Replylist="User-Name = "AB9812CD", Service-Type = "Framed"

5.4 AAAProxyRule

The rules that apply to a realm. The rules include the checklist and change list for Access-Request and Access-Accept messages.

Aliases	AAAProxyRule
Key	Name
Required	Name

— Name

- **Type:** Single
- **Description:** The name of AAA proxy rule.

— RequestChecklist

- **Type:** Single
- **Description:** The checklist that is applied to the Access-Request message.

Syntax:

```
expression := condition | '(' expression ')' | expression
logicalop expression
condition := avpname relop value
logicalop := '&' | '|' | '&&' | '||'
relop := '=' | '==' | '!=' | '>' | '>=' | '<' | '<=' | '?'
```

Where:



— avpname: The attribute. It can be one of the following:

User-Name, User-Password, CHAP-Password, NAS-IP-Address, NAS-Port, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-MTU, Framed-Compression, Login-IP-Host, Callback-Number, State, Called-Station-Id, Calling-Station-Id, NAS-Identifier, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, CHAP-Challenge, NAS-Port-Type, Port-Limit, Login-LAT-Port, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Server-Endpoint, Tunnel-Preference, Tunnel-Client-Endpoint, Tunnel-Private-Group-ID, Tunnel-Client-Auth-ID, Tunnel-Server-Auth-ID, NAS-IPv6-Address, Framed-Interface-Id, Framed-IPv6-Prefix, 3GPP-IMSI, 3GPP-Charging-Id, 3GPP-PDP-Type, 3GPP-CG-Address, 3GPP-GPRS-QoS-Negotiated-Profile, 3GPP-SGSN-Address, 3GPP-GGSN-Address, 3GPP-IMSI-MCC-MNC, 3GPP-GGSN-MCC-MNC, 3GPP-NSAPI, 3GPP-Selection-Mode, 3GPP-Charging-Characteristics, 3GPP-CG-IPv6-Address, 3GPP-SGSN-IPv6-Address, 3GPP-GGSN-IPv6-Address, 3GPP-SGSN-MCC-MNC, 3GPP-IMEISV, 3GPP-RAT-Type, 3GPP-User-Location-Info, 3GPP-MS-TimeZone, 3GPP-CAMEL-Charging-Info, 3GPP-Negotiated-DSCP, System-Time

— relop: The relational operator.

— logicalop: The logical operator.

For example: RequestChecklist="System-Time >= "10:00 +0800" && System-Time <= "20:00 +0800" && (User-Name = "User1" && (Service-Type = "Framed" || Service-Type = "Login"))"

— ReplyChecklist

- **Type:** Single
- **Description:** The checklist that is applied to the Access-Accept message.

Syntax:

```
expression := condition | '(' expression ')' | expression
logicalop logicalop expression
condition := avpname relop value
logicalop := '&' | '|' | '&&' | '||'
relop := '=' | '==' | '!=' | '>' | '>=' | '<' | '<=' | '?'
```

Where:

— avpname: The attribute. It can be one of the following:

User-Name, Service-Type, Framed-Protocol, Framed-IP-Address, Framed-IP-Netmask, Framed-Routing, Filter-Id, Framed-MTU, Framed-Compression, Login-IP-Host, Login-Service, Login-TCP-Port, Reply-Message, Callback-Number, Callback-Id, Framed-Route, Framed-IPX-Network, State, Class, Session-Timeout, Idle-Timeout, Te



termination-Action, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Framed-AppleTalk-Link, Framed-AppleTalk-Network, Framed-AppleTalk-Zone, Port-Limit, Login-LAT-Port, 3GPP-IPv6-DNS-Servers, ERICSSON-Prim-Rule-Space-Name, ERICSSON-Sec-Rule-Space-Name, ERICSSON-ACG-ID, ERICSSON-Authorization-Code, MS-Primary-DNS-Server, MS-Secondary-DNS-Server, MS-Primary-NBNS-Server, MS-Secondary-NBNS-Server, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Password, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Preference, Tunnel-Client-Auth-ID, Tunnel-Server-Auth-ID, Framed-Pool, Framed-IPv6-Prefix, Framed-IPv6-Pool, System-Time, Login-IPv6-Host, Framed-IPv6-Route, Framed-IPv6-Pool.

- relop: The relational operator.
- logicalop: The logical operator.

For example: ReplyChecklist="System-Time >= "10:00 +0800" && System-Time <= "20:00 +0800" && (User-Name = "User1" && (Service-Type = "Framed" || Service-Type = "Login"))"

— RequestChangelist

- **Type:** Multiple
- **Description:** The change list that is applied to the Access-Request message's attributes, including add, delete and replace one or more attributes.

Syntax:

```
expression := condition
condition := add:avpname="value";delete:avpname="value";replace:avpname="oldvalue:newvalue"
```

- To add an attribute with a new value, the format is:

```
add:attribute=value
```

- To delete an attribute with a value, the format is:

```
delete:attribute=value
```

- To delete an attribute with any value, the format is:

```
delete:attribute=*
```

- To replace an attribute from old value to new value, the format is:

```
replace:attribute=oldvalue:newvalue
```

Where:

- attribute: The attribute. It can be one of the following:



User-Name,NAS-IP-Address,NAS-Port,Service-Type,Framed-Protocol,Framed-IP-Address,Framed-IP-Netmask,Framed-MTU,Framed-Compression,Login-IP-Host,Callback-Number,State,Called-Station-Id,Calling-Station-Id,NAS-Identifier,Login-LAT-Service,Login-LAT-Node,Login-LAT-Group,CHAP-Challenge,NAS-Port-Type,Port-Limit,Login-LAT-Port,3GPP-IMSI,3GPP-Charging-ID, 3GPP-PDP-Type,3GPP-CG-Address,3GPP-GPRS-Negotiated-QoS-Profile,3GPP-SGSN-Address,3GPP-GGSN-Address,3GPP-IMSI-MCC-MNC, 3GPP-GGSN-MCC-MNC,3GPP-NSAPI,3GPP-Selection-Mode,3GPP-Charging-Characteristics,3GPP-CG-IPv6-Address,3GPP-SGSN-IPv6-Address,3GPP-GGSN-IPv6-Address,3GPP-SGSN-MCC-MNC,3GPP-IMEISV,3GPP-RAT-Type,3GPP-User-Location-Info,3GPP-MS-TimeZone,3GPP-CAMEL-Charging-Info,3GPP-Negotiated-DSCP,Tunnel-Client-Endpoint,Tunnel-Server-Endpoint,Tunnel-Private-Group-ID,Tunnel-Preference,Tunnel-Client-Auth-ID,Tunnel-Server-Auth-ID,NAS-IPv6-Address,Framed-Interface-Id,Framed-IPv6-Prefix

For example: RequestChangelist="add:Service-Type="Framed";add:NAS-Port-Type="Sync";delete:Port-Limit="*";replace:Callback-Number="123:456"

— ReplyChangelist

- **Type:** Multiple
- **Description:** The change list that is applied to Access-Accept message's attributes, including add, delete and replace one or more attributes.

Syntax:

```
expression := condition
condition := add:avpname="value";delete:avpname="value";replace:avpname="oldvalue:newvalue"
```

— To add an attribute with a new value, the format is:

```
add:attribute=value
```

— To delete an attribute with a value, the format is:

```
delete:attribute=value
```

— To delete an attribute with any value, the format is:

```
delete:attribute=*
```

— To replace an attribute from old value to new value, the format is:

```
replace:attribute=oldvalue:newvalue
```

Where:

— attribute: The attribute. It can be one of the following:



User-Name,Service-Type,Framed-Protocol,Framed-IP-Address,Framed-IP-Netmask,Framed-Routing,Filter-Id,Framed-MTU,Framed-Compression,Login-IP-Host,Login-Service,Login-TCP-Port,Reply-Message,Callback-Number,Callback-Id,Framed-Route,Framed-IPX-Network,State,Class,Session-Timeout,Idle-Timeout,Termination-Action,Login-LAT-Service,Login-LAT-Node,Login-LAT-Group,Framed-AppleTalk-Link,Framed-AppleTalk-Network,Framed-AppleTalk-Zone,Port-Limit,Login-LAT-Port,3GPP-IPv6-DNS-Servers,ERICSSON-Prime-Space-Name,ERICSSON-Sec-Rule-Space-Name,ERICSSON-ACG-ID,ERICSSON-Authorization-Code,MS-Primary-DNS-Server,MS-Secondary-DNS-Server,MS-Primary-NBNS-Server,MS-Secondary-NBNS-Server,Tunnel-Type,Tunnel-Medium-Type,Tunnel-Client-Endpoint,Tunnel-Server-Endpoint,Tunnel-Private-Group-ID,Tunnel-Assignment-ID,Tunnel-Preference,Tunnel-Client-Auth-ID,Tunnel-Server-Auth-ID,Framed-Pool,Framed-IPv6-Prefix,Framed-IPv6-Pool

For example: ReplyChangelist="add:Service-Type="Framed";add:NAS-Port-Type="Sync";delete:Port-Limit="*";replace:Callback-Number="123:456" "

5.5 AAAR realm

The configured policy for a realm.

Aliases	AAAR realm
Key	Name
Required	Name, AuthDest, AcctDest

— Name

- **Type:** Single
- **Description:** The name of the realm.

— StripRealm

- **Type:** Single
- **Description:** Field that decides if the realm should be stripped from the User-Name.

— AuthDest

- **Type:** Multiple
- **Description:** The IP address of next node for Radius Access-Request proxy message.

Note: If the users want to realize the local authentication, must configure the **AuthDest** as local.

**AcctDest**

- **Type:** Multiple
- **Description:** The IP address of next node for Radius Accounting-Request proxy message.
Note: If the users want to realize the local authentication, must configure the **AcctDest** as local.

ProxyRule

- **Type:** Multiple
- **Description:** The AAAProxyRule object that belongs to the realm.

5.6 AAAServer

The Authentication Authorization Accounting Server running on the network.

Aliases AAAServers

Key Name

Required Name

— **Name**

- **Type:** Single
- **Description:** The name of the AAA server. This is a unique identifier for this server.

— **Status**

- **Type:** Single
- **Description:** The last known operational status of the server.

— **Address**

- **Type:** Multiple
- **Description:** The address list associated with the server. When server manager is running, the address cannot be deleted but can be modified.

5.7 AAASession

The dynamic session in the AAA server. The session is related to a series of related Radius message exchanging, and it is used to record and update the key information according to different Radius messages. When authentication



or authorization turns to success for a user, a session will be created with init status. Accounting-Start message will be used to activate and update the session. The related sessions will be destroyed if the message is Accounting-Stop, Accounting-On, or Accounting-Off. DM will destroy the related sessions as well.

Aliases	AAASession
Key	UniqueSessionId
Required	UniqueSessionId,NasIpAddr,NasId,NasType,AcctSessionId,Class

— **UniqueSessionId**

- **Type:** Single
- **Description:** The unique session id that identifies each session.

— **NasIpAddr**

- **Type:** Single
- **Description:** It is used to record the source of the session. It is using the order preference:
 - Radius attribute NAS-IP-Address (or NAS-IPv6-Address, if available);
 - actual IPv4 (or IPv6, if available) address from which the TCP/IP packet was sent.

— **NasId**

- **Type:** Single
- **Description:** The Radius NAS-Identifier attribute value. This is used to record the source of the session. It adopts the order preference:
 - 1 Radius attribute NAS-IP-Address (or NAS-IPv6-Address, if available);
 - 2 Radius attribute NAS-Identifier;
 - 3 Actual IPv4 (or IPv6, if available) address from which the TCP/IP packet was sent.

— **NasType**

- **Type:** Single
- **Description:** It is used to record the type of the NAS. It can be one of the following:
 - Radius attribute NAS-IP-Address (or NAS-IPv6-Address, if available);
 - Radius attribute NAS-Identifier;



- actual IPv4 (or IPv6, if available) address from which the TCP/IP packet was sent.
- **AcctSessionId**
 - **Type:** Single
 - **Description:** The Radius Acct-Session-Id attribute value.
- **Class**
 - **Type:** Single
 - **Description:** The unique class value of session. It is mainly used when session is working on nasid and class model.
- **StartTime**
 - **Type:** Single
 - **Description:** The session start time.
- **Status**
 - **Type:** Single
 - **Description:** The session status value. It can only be init or active.
- **UserName**
 - **Type:** Single
 - **Description:** The Radius User-Name attribute value.
- **NasPort**
 - **Type:** Single
 - **Description:** The Radius NAS-Port attribute value.
- **FramedIpAddress**
 - **Type:** Single
 - **Description:** The Radius Framed-IP-Address attribute value.
- **FramedNetmask**
 - **Type:** Single
 - **Description:** The Radius Framed-IP-Netmask attribute value.
- **IpAllocPool**
 - **Type:** Single



- **Description:** The name of the pool that allocates on IP address.
- **IPv6PrefixPool**
 - **Type:** Single
 - **Description:** The name of the pool that can allocation IPv6 prefix.
- **CalledStationId**
 - **Type:** Single
 - **Description:** The Radius Called-Station-Id attribute value.
- **CallingStationId**
 - **Type:** Single
 - **Description:** The Radius Calling-Station-Id attribute value.
- **OriginatingLineInfo**
 - **Type:** Single
 - **Description:** The Radius Originating-Line-Info attribute value. Reserved for future use.
- **AcctMultiSessionId**
 - **Type:** Single
 - **Description:** The Radius Acct-Multi-Session-Id attribute value. If there are multiple Acct-Multi-Session-Id values, they will be separated by commas.
- **NasPortId**
 - **Type:** Single
 - **Description:** The Radius NAS-Port-Id attribute value.
- **ChargeableUserIdentity**
 - **Type:** Single
 - **Description:** The Radius Chargeable-User-Identity attribute value.
- **FramedInterfaceId**
 - **Type:** Single
 - **Description:** The Radius Framed-Interface-Id attribute value.
- **FramedIPv6Prefix**
 - **Type:** Single



- **Description:** The Radius Framed-IPv6-Prefix attribute value. If there are multiple Framed-IPv6-Prefix values, they will be separated by commas.

— **AccessAuthenticator**

- **Type:** Single
- **Description:** The Radius authenticator of Access-Request message.

— **SourceIp**

- **Type:** Single
- **Description:** The IP address of the source that send the request message.

— **ProxyDestIp**

- **Type:** Single
- **Description:** The IP address of the proxy target.

— **ProxyAcctId**

- **Type:** Single
- **Description:** The Acct-Session-Id in the message that will be forwarded to the next target.

— **ProxyClass**

- **Type:** Single
- **Description:** The Class Attribute that is received in the Access-Accept message from the proxy target.

— **LastUpdateTime**

- **Type:** Single
- **Description:** The LastUpdateTime Attribute that indicates the session last update time.

— **NeedUpdate**

- **Type:** Single
- **Description:** The NeedUpdate attribute that indicates if this session needs to be updated periodically by NAS It can be 1(needed) or 0(not needed).

— **Auth**

- **Type:** Single
- **Description:** The session auth value which indicates it has authorized. It can only be true or false.



5.8 AAASubnet

A subnet represents a contiguous set of addresses. Subnets can be split into other subnets, creating a hierarchy of subnets.

Key	Name
Required	Name, Address, Mask, MaskLength

— Name

- **Type:** Single
- **Description:** The name of the subnet.

— Address

- **Type:** Single
- **Description:** The address of the subnet.

— Mask

- **Type:** Single
- **Description:** The subnet mask for this subnet.

— MaskLength

- **Type:** Single
- **Description:** The subnet mask length for this subnet. This is a value between 0 and 32 indicating the number of bits that are set in the mask.

5.9 AAAtempIdentityKey

Aliases	AAAtempIdentityKey
Required	KeyValue, suspendedKeyNumber

— KeyValue

- **Type:** Single
- **Description:** this is used to generate temporary identity.

— SuspendedKeysNumber

- **Type:** Single
- **Description:** this is used to limit valid historical keyValue number. Its value should be between 1 and 15.



5.10 AAAUser

The AAA user information.

Aliases	AAAUser
Key	Username
Required	Username, Password

— Username

- **Type:** Single
- **Description:** The user name of the user.

For Fixed Access IPoE users, this parameter means the access loop ID value. The value is a string, which can be one AVP or a combination of multiple AVPs from the following:

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

— Password

- **Type:** Single
- **Description:** The password of the user.

— AuthMethod

- **Type:** Single
- **Description:** The authentication method used for this user. It can be EAP-MD5, EAP-SIM/AKA.

— Policy

- **Type:** Multiple
- **Description:** The names of policy. The user may have multiple policies.

— IPAllocType

- **Type:** Single



- **Description:** The policy of IP address allocation. There are 4 types:
 - 0: Default value. Assign IP address from the Radius client related IP address pool(s) if the attribute Framed-IP-Address is contained in Access-Request message , otherwise don't assign IP address.
 - 1: Static assignment - The attribute IPAllocValue should be set using a static IP address. And this IP will be assigned each time to the user .
 - 2: Assign IP from a specific IP address pool - The attribute IPAllocValue should be set using an existent AAAIPPool. And one available IP address from this specific IP pool will be assigned.
 - 3: Assign IP from the Radius client related IP address pool(s) - The attribute IPAllocValue doesn't need any value (even if configured, server will not care). An address will be assigned from one of the pools associated with the Radius client based on APN selection .
- **IPAllocValue**
 - **Type:** Single
 - **Description:** The value which defines the IP address will be allocated from which pool or address.
 - If the IPAllocType is 0 or 3, the default value of IPAllocValue is 0, which is meaningless.
 - If the IPAllocType is 1, the IPAllocValue must be in the format of <IP Address>/<netmask length>, for example, 10.0.0.1/24. If the netmask length is not assigned, the Framed-IP-Netmask 255.255.255.255 will be returned to the client.
 - If the IPAllocType is 2, the IPAllocValue must be the name of the AAAIPPool that is created by user.
- **IPv6PrefixAllocType**
 - **Type:** Single
 - **Description:** The mode of IPv6 prefix allocation. There are 4 types:
 - 0: Default value. Assign IPv6 prefix from the Radius client related IPv6 prefix pool(s) if the attribute Framed-IPv6-Prefix is contained in Access-Request message, otherwise don't assign IPv6 prefix.
 - 1: Static assignment - The attribute IPv6PrefixAllocValue should be set using a static IPv6 prefix. And this IPv6 prefix will be assigned each time to the user.
 - 2: Assign IPv6 prefix from a specific IPv6 prefix pool - The attribute IPv6PrefixAllocValue should be set using an existent AAAIPv6PrefixPool. And one available IPv6 prefix from this specific IPv6 prefix pool will be assigned.



- 3: Assign IPv6 prefix from the Radius client related IPv6 prefix pool(s) - The attribute IPv6PrefixAllocValue doesn't need any value (even if configured, server will not care). An IP address will be assigned from one of the pools associated with Radius client or the Radius client based on APN selection.
- **IPv6PrefixAllocValue**
 - **Type:** Single
 - **Description:** The value which defines the IPv6 prefix will be allocated from which pool or IPv6 prefix.
 - If the IPv6PrefixAllocType is 0 or 3, the default value of IPv6PrefixAllocValue is 0, which is meaningless.
 - If the IPv6PrefixAllocType is 1, the IPv6PrefixAllocValue must be in the format of <IPv6 ADDRESS>/<length>, for example, 2012:ABCD:170:29::/64.
 - If the IPv6PrefixAllocType is 2, the IPv6PrefixAllocValue must be the name of the AAAIPv6PrefixPool that is created by user.
- **IMSI**
 - **Type:** Single
 - **Description:** International Mobile Subscriber Identity of the user.

Note: IMSI is only used for the Secure SSID feature.

5.11 AAANSUser

The AAA Non-Sim Device User information.

Aliases	AAANSUser
Key	Name
Required	Name, IMSI, MSISDN, userStatus

- **Name**
 - **Type:** Single
 - **Description:** The user name of the user.
- **IMSI**
 - **Type:** Single
 - **Description:** International mobile subscriber identify of user.
- **MSISDN**



- **Type:** Single
 - **Description:** Mobile Station international ISDN number of user.
- **APN**
- **Type:** Single
 - **Description:** Access Point Name list for the Non-SIM devices.
- **userStatus**
- **Type:** Single
 - **Description:** The user status:
 - Enable: Enable the user.
 - Disable: Disable the user.
- **Password**
- **Type:** Single
 - **Description:** The password of the User.
- **certificateid**
- **Type:** Single
 - **Description:** Certificate Id of user certificate. For more information, refer to Section 4.1.2.2 Serial Number in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Reference [21]. Possible value:
 - A decimal positive integer. For example, 8125922033436420856
 - Empty, which means the certificate of this user is invalid.
- **certificateissuename**
- **Type:** Single
 - **Description:** Certificate Issuer Name of user certificate.

For information about the certificateissuename format, refer to Section 5.1.2.3 Issuer Name in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Reference [21].

The Issuer Name is split by comma (,) and a blank space:

For example, certificateissuename="CN=AdminCA1, O=EJBCA Sample, C=SE"



If the Issuer Name is empty, it means that the certificate of the user is invalid.

5.12 AAAUserGroup

The user group.

Aliases AAAGroup

Key Name

Required Name

— Name

- **Type:** Single
- **Description:** The name of the group.

— Policy

- **Type:** Multiple
- **Description:** The names of policy. The group may have multiple policies.



6 Appendix

6.1 Example of Configuring 3GPP-User-Location-Info

When the users get the network information, for example, if the Geographic Location type is SAI(1), the MCC is 460, the Mobile Networks Code(MNC) is 13, LAC is 1007, and SAC is 0001, then users must perform the following steps:

1. Convert the network information to the 3GPP-User-Location-Info octet string hex.

For the detailed algorithm, refer to 3GPP TS 29601 and 3GPP TS 29274.

For example:

Users get the 3GPP-User-Location-Info octet string 0164f03103ef0001 according to the following table.

Geographic Location Type	MCC digit 2	MCC digit 1	MNC digit 3	MCC digit 3	MNC digit 2	MNC digit 1	Location Area Code (LAC)	Service Area Code (SAC)
01	6	4	f	0	3	1	03ef	0001

```

AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
AVP: l=16 t=Vendor-Specific(26) v=3GPP(10415)
VSA: l=10 t=3GPP-User-Location-Info(22): 0164f03103ef0001
  Geographic Location Type: 1
  Mobile Country Code (MCC): China (People's Republic of) (460)
  Mobile Network Code (MNC): unknown (13)
  Cell LAC: 0x03ef (1007)
  SAC: 0x0001

```

2. Convert the hex to format string ('dec dec dec...').

Configure the 3GPP-User-Location-Info as '1 100 240 49 3 239 0 1' '01 64 f0 31 03 ef 00 01' => '1 100 240 49 3 239 0 1'.





Reference List

IPWorks Documents

- [1] Command Line Interface User Guide for IPWorks SS
- [2] Glossary of Terms and Acronyms
- [3] Trademark Information
- [4] Typographic Conventions
- [5] Configure Radius AAA

Standards

- [6] [Microsoft Vendor-specific RADIUS Attributes](#)
- [7] [Remote Authentication Dial In User Service \(RADIUS\)](#)
- [8] [RADIUS Accounting](#)
- [9] [RADIUS Accounting Modifications for Tunnel Protocol Support](#)
- [10] [RADIUS Attributes for Tunnel Protocol Support](#)
- [11] [RADIUS Extensions](#)
- [12] [RADIUS and IPv6](#)
- [13] [Diameter Base Protocol](#)
- [14] [Chargeable User Identity](#)
- [15] [RADIUS Attributes for Virtual LAN and Priority Support](#)
- [16] [RADIUS Delegated-IPv6-Prefix Attribute](#)
- [17] [RADIUS Filter Rule Attribute](#)
- [18] [Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\)](#)
- [19] [3GPP TS 29.061 Version 8.2.0 Release 8](#)
- [20] [Internet Message Format](#)
- [21] [Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile](#)