RADIUS

remote authentication dial in user service

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

Radius is a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server (NAS) that desires to authenticate its links and a shared Authentication Server.

This tutorial starts off with an overview of Radius followed by its features, operations, packet format, and attributes. Subsequently, the tutorial provides a few examples of Radius request and response, and terminates with a brief introduction to Diameter, a planned replacement of Radius.

Audience

This is an introductory tutorial designed for beginners to help them understand the basics of Radius.

Prerequisites

There are no prerequisites as such, however it would help if you have a basic understanding of client/server environment.

Copyright & Disclaimer

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

1. AAA AND NAS

Before you start learning about Radius, it is important that you understand:

- What is AAA?
- What is NAS?

So let us first have a basic idea about these two topics.

What is AAA?

AAA stands for Authentication, Authorization, and Accounting.

Authentication

- Refers to confirmation that a user who is requesting a service is a valid user.
- Accomplished via the presentation of an identity and credentials.
- Examples of credentials include passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization

- Refers to the granting of specific types of service (including "no service") to the users based on their authentication.
- May be based on restrictions, for example, time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user.
- Examples of services include IP address filtering, address assignment, route assignment, encryption, QoS/differential services, bandwidth control/traffic management, etc.

Accounting

- Refers to the tracking of the consumption of network resources by users.
- Typical information that is gathered in accounting include the identity of the user, the nature of the service delivered, when the service began, and when it ended.
- May be used for management, planning, billing, etc.

AAA server provides all the above services to its clients.

AAA Protocols

Radius is an AAA protocol for applications such as Network Access or IP Mobility. Besides Radius, we have the following protocols in AAA:

Terminal Access Controller Access Control System (TACACS)

TACACS is a remote authentication protocol that is used to communicate with an authentication server commonly used in Unix networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

TACACS+

TACACS+ provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. It uses TCP and provides separate authentication, authorization, and accounting services. It works on port 49.

DIAMETER

Diameter is a planned replacement of Radius.

What is Network Access Server?

The Network Access Server (NAS) is a service element that clients dial in order to get access to the network. An NAS is a device having interfaces both to the backbone and to the POTS or ISDN, and receives calls from hosts that want to access the backbone by dialup services. NAS is located at an Internet provider's point of presence to provide Internet access to its customers.

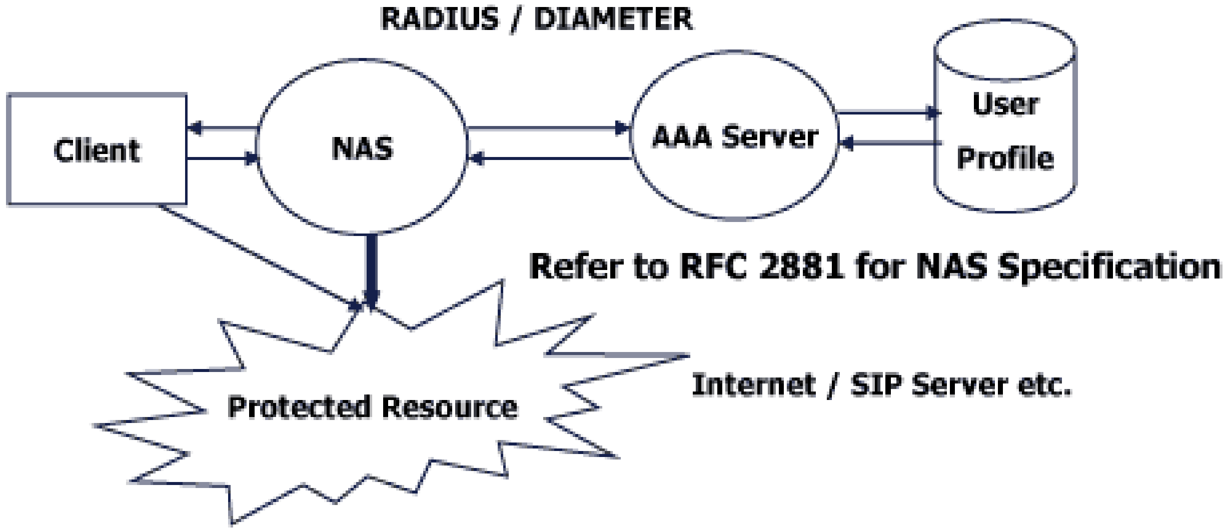
A Network Access Server is:

- A single point of access to a remote resource.
- A Remote Access Server, because it allows remote access to a network.
- An Initial Entry Point to a network.
- A Gateway to guard to protected resource.

Examples include:

- Internet Access Verification using User ID and Password.
- VoIP, FoIP, and VMoIP require a valid Phone Number or IP Address.
- Telephone Prepaid Card uses Prepaid Card Number.

The following figure shows a basic architecture of Radius.


RADIUS / DIAMETER
Client
NAS
AAA Server
User
Profile
Refer to RFC 2881 for NAS Specification
Protected Resource
Internet / SIP Server etc.

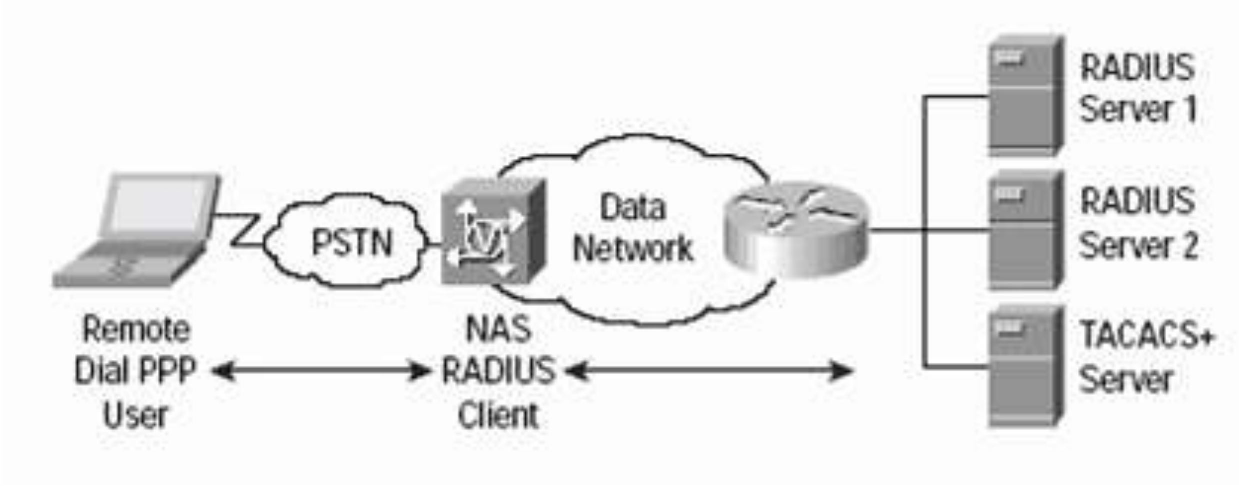
Basic Architecture for NAS/RADIUS/AAA

2. OVERVIEW

RADIUS is a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

- RADIUS stands for Remote Authentication Dial In User Service.
- RADIUS is an AAA protocol for applications such as Network Access or IP Mobility.
- It works in both situations, local and mobile.
- It uses Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) protocols to authenticate users.
- It looks in text file, LDAP Servers, or Database for authentication.
- After authentication, service parameters are passed back to NAS.
- It notifies when a session starts and stops. This data is used for Billing or Statistics purposes.
- SNMP is used for remote monitoring.
- It can be used as a proxy.

Here is a simple Network Diagram of Radius:



3. FEATURES

Here is a list of all the key features of Radius:

Client/Server Model

- NAS works as a client for the Radius server.
- Radius server is responsible for getting user connection requests, authenticating the user, and then returning all the configuration information necessary for the client to deliver service to the user.
- A Radius server can act as a proxy client to other Radius servers.

Network Security

- Transactions between a client and a server are authenticated through the use of a shared key. This key is never sent over the network.
- Password is encrypted before sending it over the network.

Flexible Authentication Mechanisms

Radius supports the following protocols for authentication purpose:

- Point-to-Point Protocal - PPP
- Password Authentication Protocol - PAP
- Challenge Handshake Authentication Protocol - CHAP
- Simple UNIX Login

Extensible Protocol

Radius is extensible; most vendors of Radius hardware and software implement their own dialects.

Stateless protocol, using UDP, runs at port 1812.

4. OPERATIONS

Before the Client starts communicating with the Radius Server, it is required that the secret key is shared between the Client and the Server and the Client must be configured to use Radius server to get service.

- The Client starts with Access-Request.
- The Server sends either Access-Accept, Access-Reject, or Access-Challenge.
- Access-Accept keeps all the required attributes to provide service to the user.

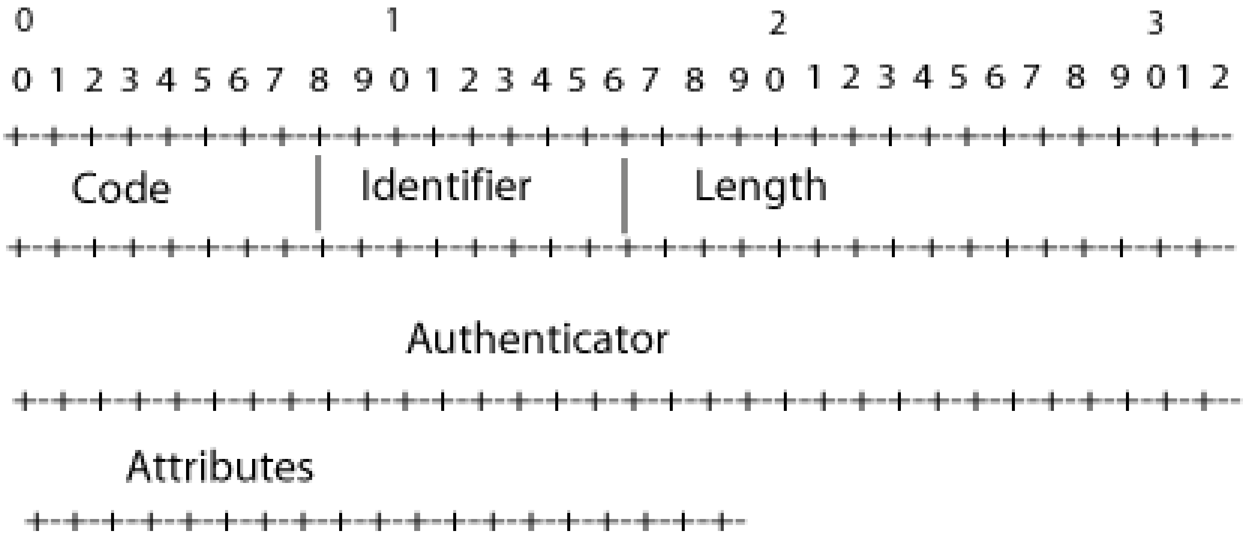
Radius Codes (decimal) are assigned as follows:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 255 Reserved
- No Keep Alive concept - Good or Bad??

Codes 4 and 5 are related to Radius Accounting Functionality. Codes 12 and 13 are reserved for possible use.

5. PACKET FORMAT

The packet format of Radius is as shown below:



Code: This is 1 Octet (1 byte) long and identifies various types of packets. Normally 1 Octet means 1 Byte.

Identifier: This is again 1 Octet long and aids in matching responses with requests.

Length: This is 2 Octets long and specifies the length of the packet including code, identifier, length, and authenticator. (Min packet is 20 Octets and max is 4096 Octets).

Authenticator: This is 16 Octets long and filled up in case of some requests and responses.

List of Attributes: There is a list of 63+ attributes and a Radius attribute will also have a defined format which is described in next chapter.

6. ATTRIBUTES LIST

A Radius attribute consists of the following three parts:

- **Type:** 1 Octet long, identifies various types of attributes. It is an attribute code listed below.
- **Length:** 1 Octet long, length of the attribute including Type.
- **Value:** 0 or more Octets long, contains information specific to attribute.

RADIUS Attributes List

Code	Attributes	Code	Attributes
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node 3
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40 - 59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge

20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

7. EXAMPLES

Radius Request Example

Let us have a look into a Radius Request example:

- The NAS at 192.168.1.16 sends an Access-Request UDP packet to the RADIUS Server for a user named Nemo logging in on port 3 with password "arctangent".

- The Request Authenticator is a 16 octet random number generated by the NAS.
- The User-Password is 16 octets padded at end with nulls, XORed with D5 (Shared Secret|Request Authenticator).

- 01 00 00 38 0f 40 3f 94 73 97 80 57 bd 83 d5 cb 98 f4 22 7a 01 06 6e 65 6d 6f 02 12 0d be 70 8d 93 d4 13 ce 31 96 e4 3f 78 2a 0a ee 04 06 c0 a8 01 10 05 06 00 00 00 03

- 1 Code = Access-Request (1)

  1 Identifier = 0

  2 Length = 56

  16 Request Authenticator
- Attribute List

  6 User-Name = "Nemo"

  18 User-Password

  6 NAS-IP-Address = 192.168.1.16

  6 NAS-Port = 3

Radius Response Example

Here is an example of Response Packets:

- The Radius server authenticates Nemo and sends an Access-Accept UDP packet to the NAS telling it to telnet Nemo to host 192.168.1.3

- The Response Authenticator is a 16-octet MD5 checksum of the code (2), id (0), Length (38), the Request Authenticator from above, the attributes in this reply, and the shared secret.

- 02 00 00 26 86 fe 22 0e 76 24 ba 2a 10 05 f6 bf 9b 55 e0 b2 06 06 00 00 00 01 0f 06 00 00 00 00 0e 06 c0 a8 01 03

- 1 Code = Access-Accept (2)

  1 Identifier = 0 (same as in Access-Request)

  2 Length = 38

  16 Response Authenticator

- Attribute List:

  6 Service-Type (6) = Login (1)

  6 Login-Service (15) = Telnet (0)

  6 Login-IP-Host (14) = 192.168.1.3

8. DIAMETER

Diameter is a planned replacement of RADIUS. It is an AAA protocol for applications such as network access and IP mobility. Listed below are a few points that you need to know about Diameter:

- It is intended to work in both local and roaming AAA situations.
- Diameter is just twice the predecessor protocol Radius.
- It uses TCP or SCTP and not UDP.
- It uses transport level security (IPSEC or TLS).
- It has 32 bit identifier instead of 8 bit.
- It supports stateless as well as stateful mode.
- It supports application layer acknowledgement, define failover.
- It offers better roaming support.
- It uses AVPs.
- Diameter allows to define new commands and attributes. It is easy to extend.

What is Next?

Now you have a basic understanding of Radius and Diameter. To gain more knowledge about these protocols, you need to go through various RFCs and other resources mentioned in the Resources section.