Authentication, Access Control and Roaming

ORONTI ADEWALE

Radius Introduction

- Radius is a protocol that handle authentication but also authorization and accounting as well
- It Helps Centralized Authentication in networks
- Most AAA services uses RADIUS

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.

Authentication, Authorization, Accounting?

- Authentication can be posed as a question that is Who are you?
- Authorization can also be posed as a question that is What services am I allowed to give you?
- Accounting can be posed as a question that is what did you do with my services while you were using them?

What is RADIUS? - In Summary

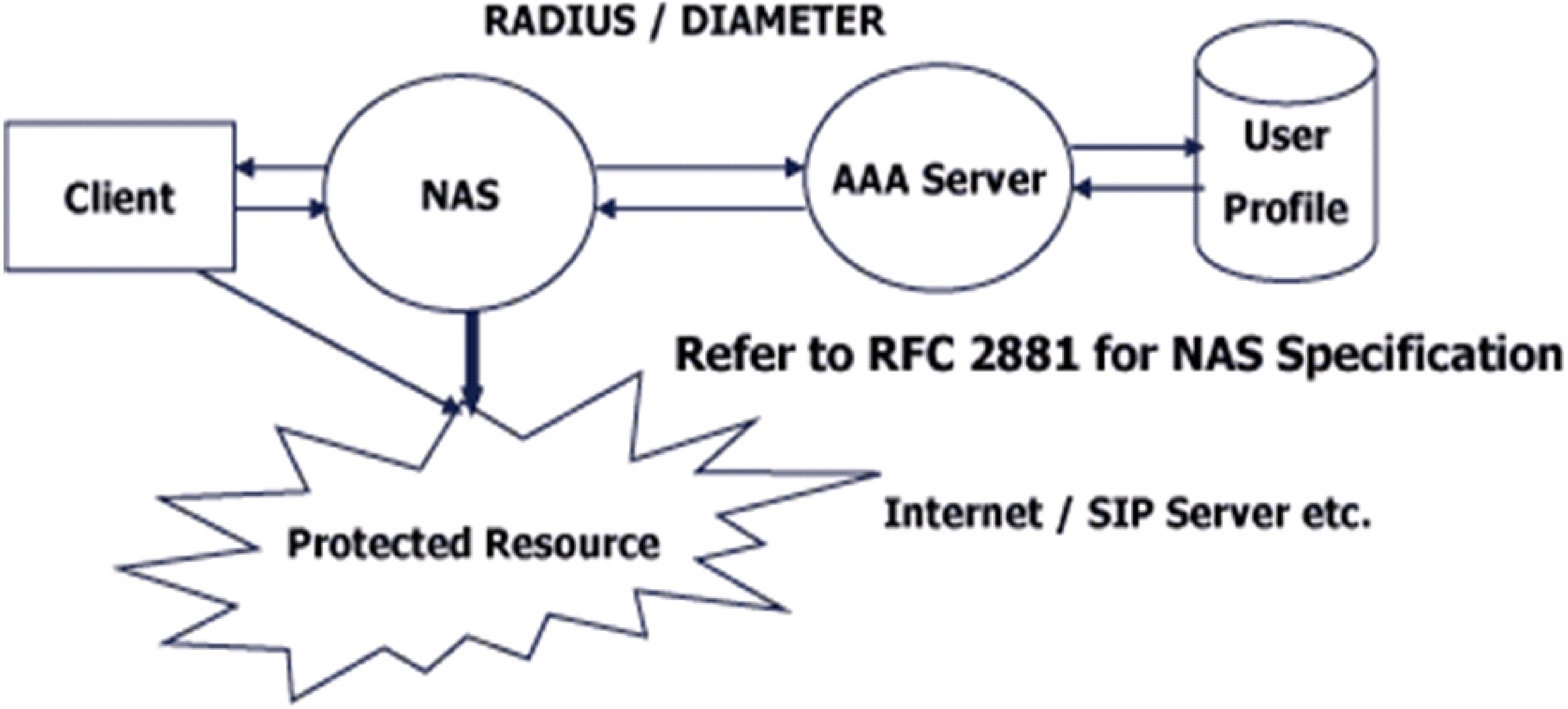
- Authentication is a process of verifying a person’s identity.

- Authorization is using a set of rules or attribute to decide what an authenticated user can do on a system

- Accounting is measuring and documenting the resources a user takes advantage of during access.

- RFC 2058, 2059 and 3865 contains more documentation on it.

Basic Architecture of NAS/Radius/AAA

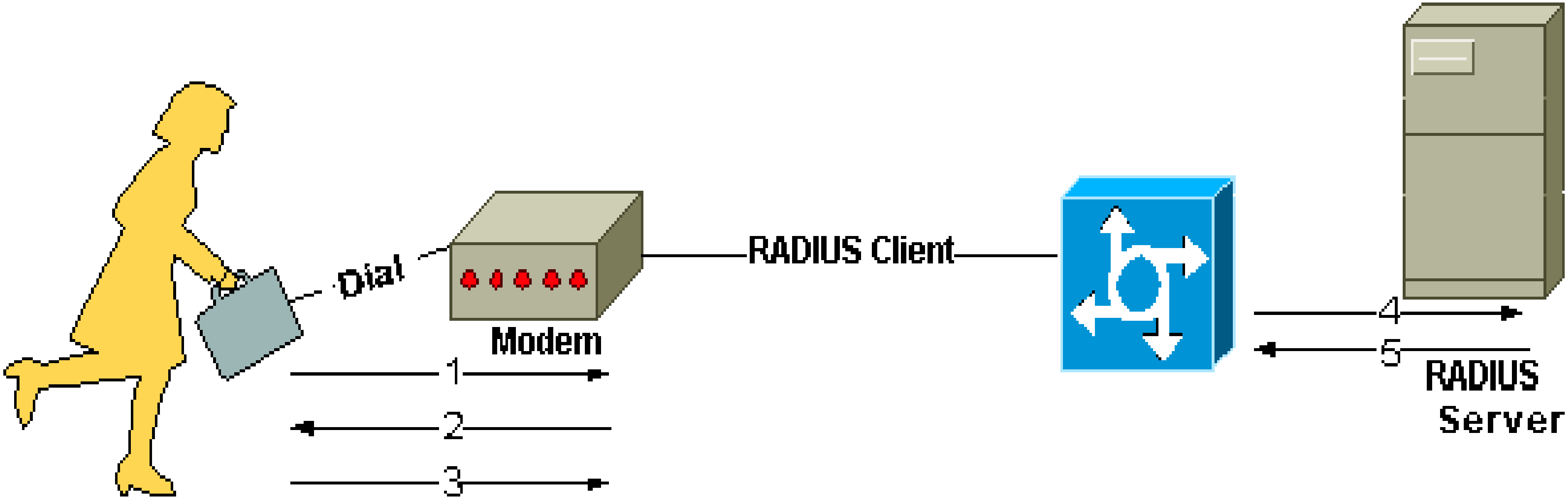


Refer to RFC 2881 for NAS Specification

Basic Architecture for NAS/RADIUS/AAA

RADIUS Mechanism

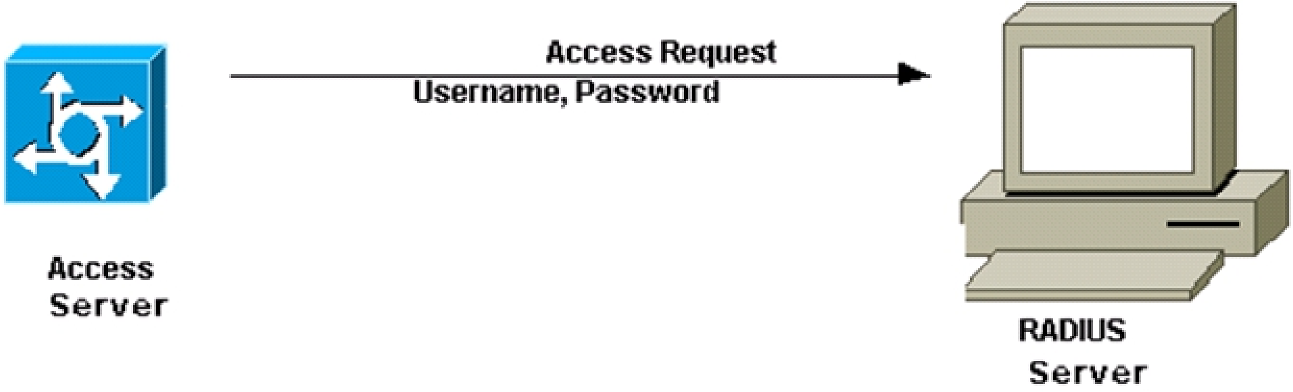
Radius in action



RADIUS Message

- Access Request

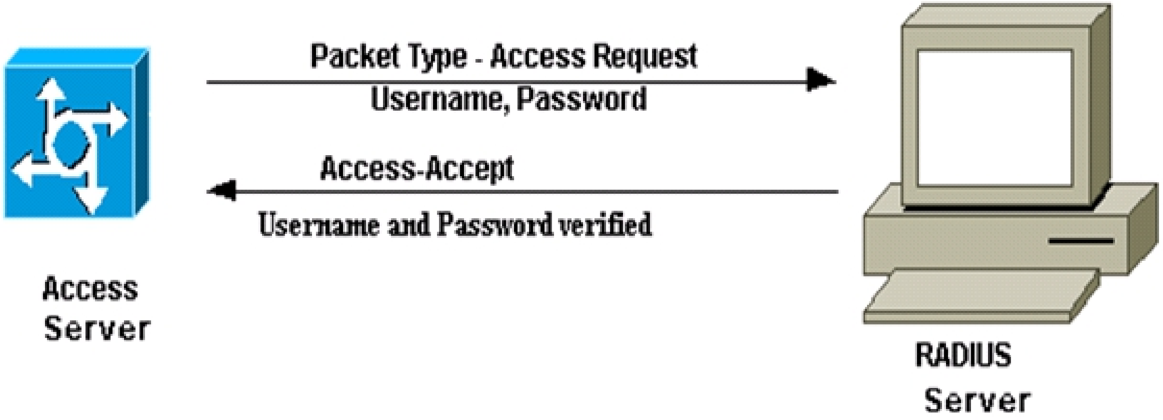
* Generated by the NAS (RADIUS client) towards the server to forward the request from or on behalf of a user.



RADIUS Message Continue

- Access Accept

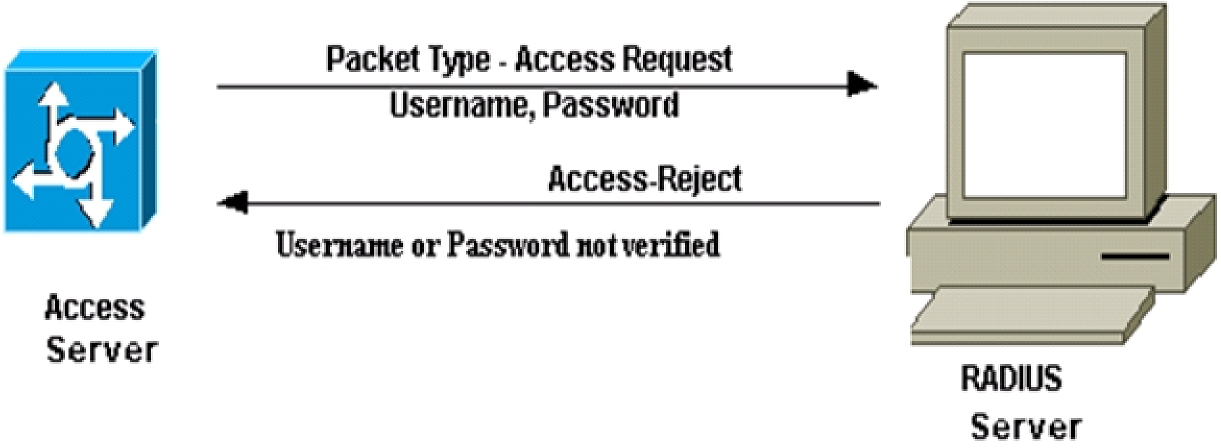
* This message is sent from the RADIUS server to the NAS to indicate a successful completion of the request



RADIUS Message continue

- Access Reject

* This message is sent by the server to indicate the rejection of a request


Packet Type - Access Request
Username, Password
Access-Reject
Username or Password not verified
Access Server
RADIUS Server

RADIUS Message Continue

- Accounting request
  - Sent from the client to the accounting server to convey accounting information regarding the service provided to the user
- Accounting response

* Sent by the server to the client (NAS) to acknowledge and indicates the result of the performed accounting function by the server

Detail Radius Operations

- Radius Codes 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

Configuring User Information

The Radius users file is a flat text file on the Radius Server. The users file stores authentication and authorization information for all users authenticated with Radius . For each user, you must create an entry that consists of three parts: the username, a list of check items, and a list of reply items.

```
 lasisi           Password = 'lusada'
                 Service-Type = Frame-User,
                 Framed-protocol = PPP,
                 Framed-IP-Address =
192.168.1.2
                 Framed-IP-Netmask =
255.255.255.255
                Framed-Routing = None,
                Framed-MTU = 1500
```

lasisi is the username and password lusada is a check item and we have Service-Type as the first Reply Item and Framed-IP-Address being the second item.

*Username

The username is the first part of each user entry. Username consist of up to 63 printable,nonspace, ASCII characters.

*Check Items

Check items are listed on the first line of a user entry, separated by commas. For an access request to succeed, all check items in the user entry must be matched in the access request.

*Reply Items

Reply items give the NAS information about the user's connection. Eg whether to use PPP or SLIP is used or whether the user's IP address is negotiated.

If all check items in the user entry are satisfied by the access-request, the radius server sends the reply items to the NAS to configure the connection.

* Password Locations

Use the Auth-Type check item to specify the type of authentication to use for a particular user. Auth-Type can be either of the following : Local , System or SecureID. If the check Item is omitted the user entry , Local is assumed.

* Local

To indicate that the user's password is stored in the Radius users file, use the Local Auth-Type. To set the user's password, use the Password check Item. An example line from a user entry is displayed below.

```
lasisi Auth-Type = Local, Password = 'lusada'
```

* System

To indicate that the user's password is stored in a system password file, use the System Auth-Type.

the RADIUS server receives a username-password pair from the client, it queries the operating system to determine if there is a matching username-password pair.

Eg.

```
lasisi                    Auth-Type = System
```

SecureID

The SecureID Auth-Type indicates that the user's password should be authenticated by a securID Server.

eg.

```
lasisi                    Auth-Type=SecurID
```

To receive a passcode from SecureID, the Server software must be running on the same unix host as the radius server.

Configuring Client Information

Use the NAS-IP-Address check item to specify the IP address of a particular NAS. When this setting is used as a check item in a user entry, the user must attempt to start a connection on the specified NAS for the connection to succeed.

Use the NAS-Port check Item to specify a particular NAS port. To be successfully authenticated, the user must attempt to log in to this port.

Use the NAS-Port-Type check item to specify the type of port. Options for the NAS-Port-Type are as follows: Async, Sync, ISDN, ISDN-V120 or ISDN-V110.

Eg display a user entry containing the NAS-IP-Address and NAS-Port-Type settings.

lasisi   Password = “lusada”, NAS-IP-Address=192.168.2.2, NAS-Port-Type = ISDN

Service-Type = Framed-User,

Framed-Protocol = PPP

Configuring Reply Items

* Service Type

You must specify the type of service provided to the user, called the Service-Type, in each user entry. Service-Type must be set to one of the values show below.

Login-User → User connects via telnet, rlogin

Framed-User → User uses PPP or SLIP for connection

Outbound-User → User uses telnet for outbound connections.

- Framed Protocol

When the service-type is a Framed-User, you must include the Framed-Protocol reply item in the user entry to indicate whether PPP or SLIP is used.

Eg for a user lasisi is a PPP user. His full entry includes the following lines below:

```
lasisi          Auth-Type = System
                Service-Type = Framed-User
                Framed-Protocol = PPP
```

* Framed IP Address

Use the Framed-IP-Address reply item to specify the user's IP address.

When Framed-IP-Address is set to 192.168.1.2, the NAS negotiates the address with the end-node (dial-in user). When it is omitted, the NAS assigns an IP address to the dial-in user from the assigned addresspool.

* Framed IP Netmask

You must specify a netmask for a user using the Framed-IP-Netmask reply item. If this reply item is omitted, the default subnet mask of 255.255.255.255 is used.

* Framed Route

Use the Framed-Route reply item to add a route to NAS routing table when service to the user begins. Three pieces of information are required: the destination IP address, gateway IP address, and metric.

Eg. is as below

```
lasisi                  Auth-type = System
                        Service-Type = Framed-User,
                        Framed-Protocol = PPP,
                        Framed-IP-Address = 196.200.219.4
                        Framed-Route = “196.200.219.0
196.200.219.4 1”
```

In this eg. 196.200.219.0 is the IP address of a destination network. 196.200.219.4 is the IP address of the gateway for this network.

N.B: If 0.0.0.0 is specified as the gateway IP address, the user's IP address is substituted for the gateway.

?