Session 2: Introduction to RADIUS and FreeRadius implementation

eduroam deployathon Workshop

Lagos, October 2024

LOCAL HOST

WITH SUPPORT FROM

Summary

Overview

Network resources protection against malicious activities requires standards, policies, and tools to enforce data protection. In TCP/IP networks a proven standard protocol (the Triple AAA) exists that is widely used on NAS. FreeRadius one of the implementation of this protocol offers:

- simplicity
- flexibility
- a lot of modules
- community support

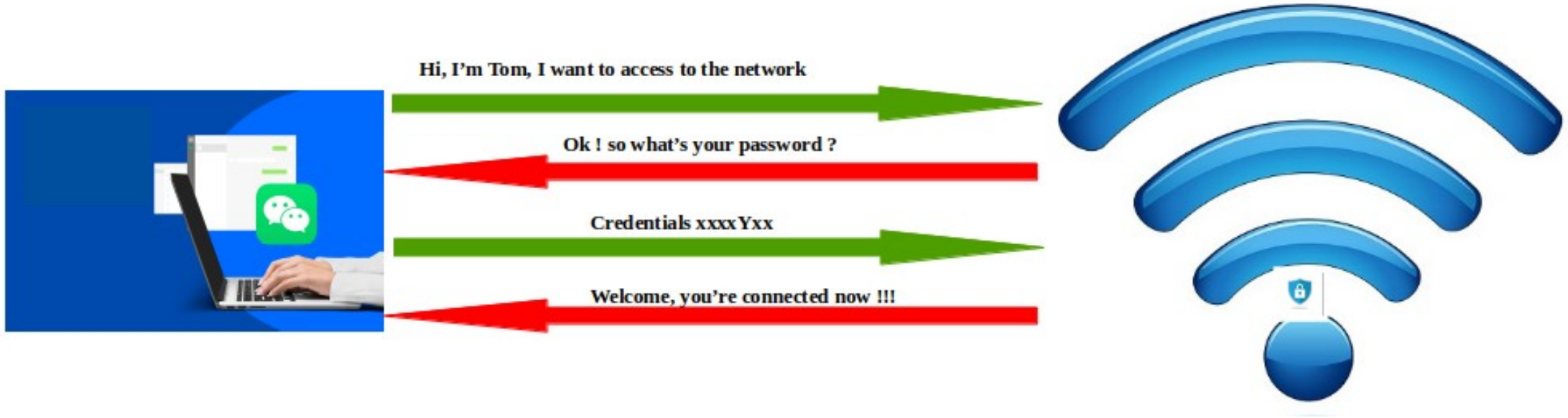
The Triple A

AAA refers to a specification (RFC 2903). The spec defines how a Network device (WiFi AP, WiFi controller, Switch) can be configure to exercise some form of Control to ensure proper security and usage.

The Triple A : Authentication

Authn: the process to check and confirm whether the credentials provided by a user are valid

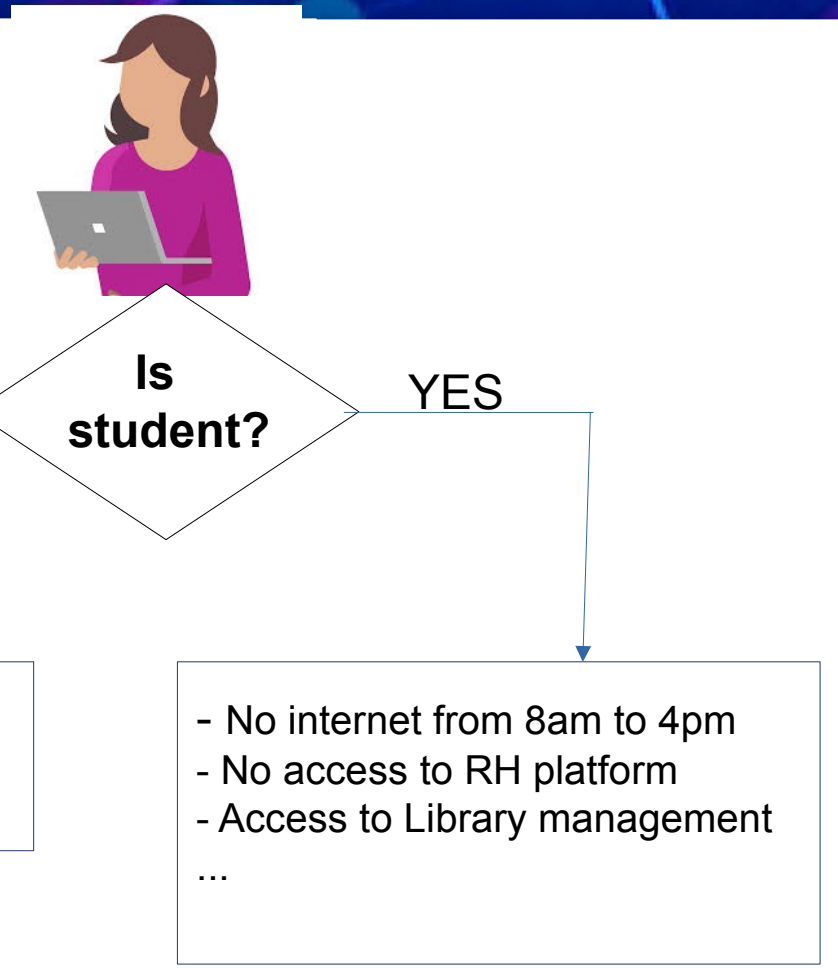
Authn→ **Validation**→ **Session initialization**



The Triple A : Authorization

Authz: is the means by which the resource owner or maintainer controls the usage of the resource

Session Initialization→ Restrictions/Granted Privileges/QoS/SLA



The Triple A : Accounting

Acct: is the mean of measuring resources consumption. After authenticating and authorizing a given user; the resource maintainer should monitor the usage

Acct→ **monitoring→ statistics→ trend→ billing→** Decision Making(analysis, capacity planning. Should we increase bandwidth ?)

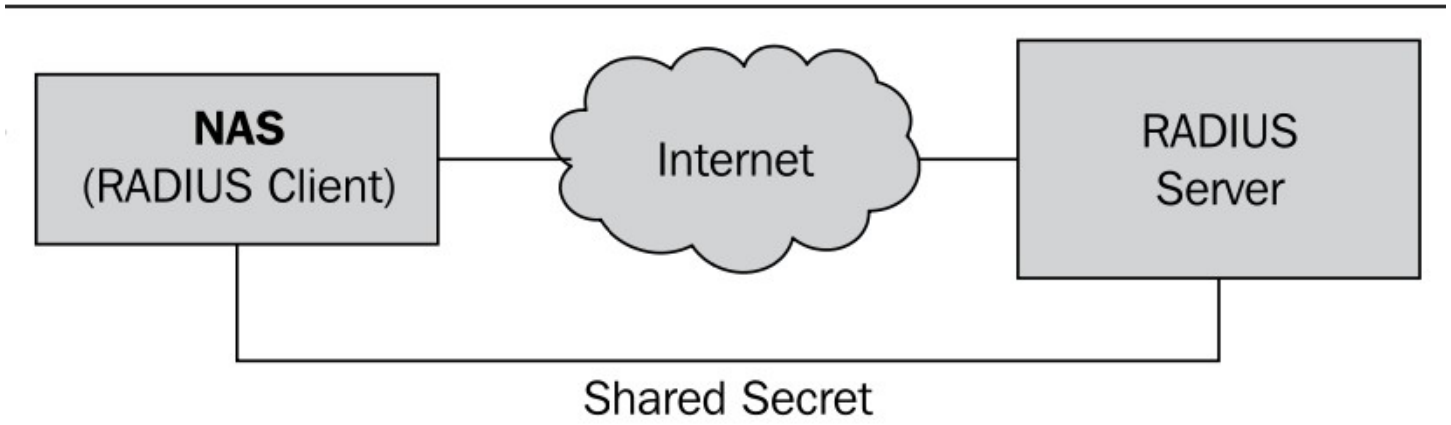
About Radius Protocol

RADIUS (Remote Access Dial in User Service) is a protocol which is used to provide AAA on TCP/IP networks. It was specified in RFCs 2865, 2866 (https://datatracker.ietf.org/doc/html/rfc2865)

The Spec defines : the protocol operation, packet format, packet types, attributes, etc.

RADIUS was widely adopted since the 1990s and supporting RADIUS becomes a defacto requirement for NAS vendors.

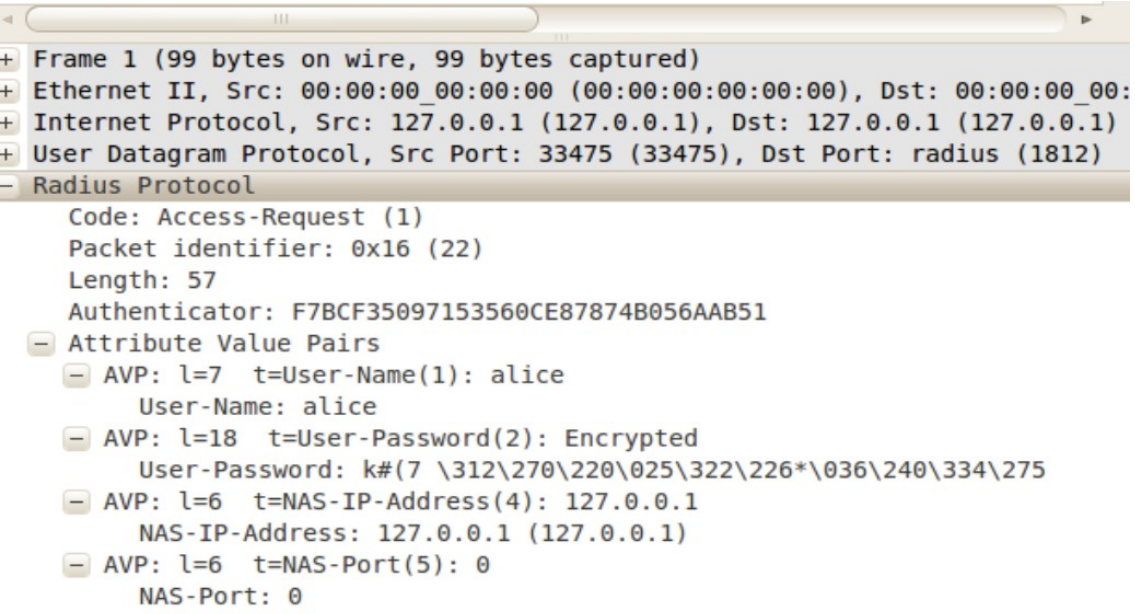
About Radius Protocol

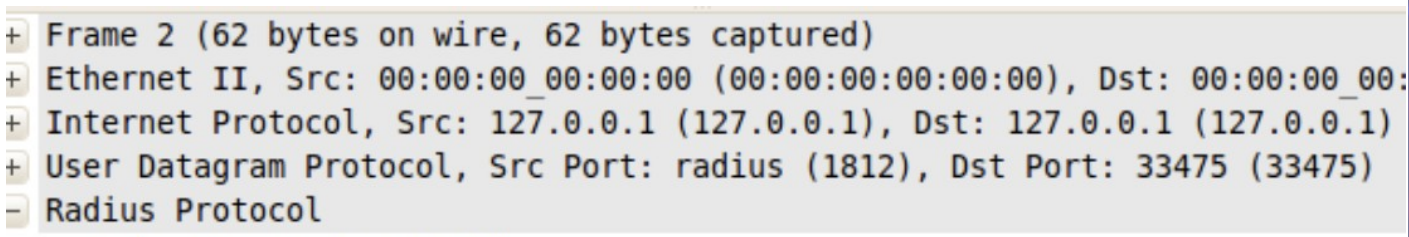


RADIUS is a client/server(port 1812 for Authn+Authz; port 1813 for Acct) protocol using udp(preferably)/tcp port for communication with **the requirement to have the 2 parties share a secret prior to any successful communication**.

About Radius Protocol

A RADIUS packet is made of 2 parts(code + attributes)





Understanding FreeRadius implementation

FreeRadius(https://www.freeradius.org , https://wiki.freeradius.org , https://deployingradius.com) is an opensource implementation of the RADIUS protocol

Its deployment is pretty simple:

- Native install : apt install freeradius

- docker: https://gitlab.wacren.net/Service/eduroam/eduroam-idp

Authn with FreeRadius

There are a number of authentication protocols available in FreeRadius: PAP, CHAP, MS-CHAP

PAP(Password Authentication Protocol): username+password send in cleartext to the NAS; encrypted and forwarded to the authentication server.

CHAP(Challenge-Handshake Authentication Protocol): NAS sends a challenge to the user. The user responds to this challenge by returning a one-way hash calculated on an identifier (sent along with the challenge), the challenge, and the user's password.

MS-CHAP(Microsoft Challenge-Handshake Authentication Protocol): A CHAP created by microsoft.

Authz with FreeRadius

Applying restrictions is done in authorize section of the virtual server based on AVPs in Access-Request packet

unlang example to deny reject any request from zombie clients

```
authorize {
        if (!&Message-Authenticator) {
                reject
        }
```

Acct under FreeRadius

Accounting refers to tracking of the consumption of NAS resources by users. Accounting does not only include cost recovery in the form of billing. It can also be used for capacity planning, to generate trend graphs, and to know more about the resource usage at a given point in time. In this chapter, we will see how accounting is done in FreeRADIUS.

Accounting-request(status=Start

Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "4D2BB8AC-00000098"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Name = "tom"
NAS-Port = 0
Called-Station-Id = "00-02-6F-AA-AA-AA:My Wireless"
Calling-Station-Id = "00-1C-B3-AA-AA-AA"
NAS-Port-Type = Wireless-802.11
Connect-Info = "CONNECT 48Mbps 802.11b"

Accounting-request(status=update

Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "4D2BB8AC-00000098"
Acct-Status-Type = Interim-Update
Acct-Authentic = RADIUS
User-Name = "tom"

Accounting-request(status=stop

Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "4D2BB8AC-00000098"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Name = "tom"
NAS-Port = 0
Called-Station-Id = "00-02-6F-AA-AA-AA:My Wireless"

Thank you!

THANKS!