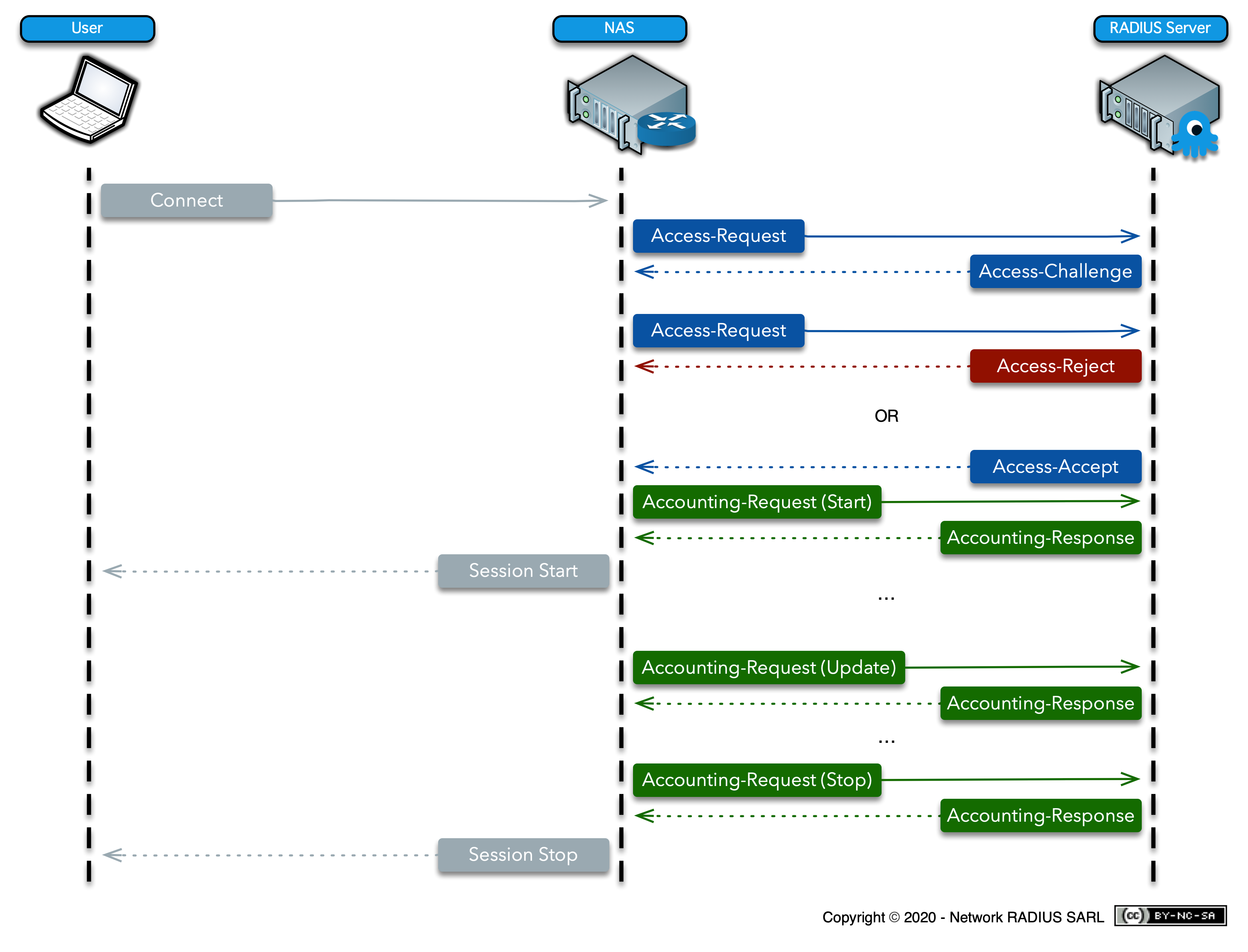
RADIUS OTP

1. OTP là gì?

* Là phương thức xác thực đăng nhập một khẩu một lần và chỉ có giá trị cho một lần đăng nhập (xác thực hai nhân tố). Mục đích để đảm bảo an toàn tài khoản cho người dùng, tránh bị đánh cắp dữ liệu. Mã OTP được sinh ra ngẫu nhiên sau thời gian nhất định.

1. Radius

* Là protocol, chuyển các yêu cầu xác thực đến một hệ thống quản lí danh tính. Theo mô hình client – server. Dùng để truy cập từ xa.
* Kiến trúc: AAA: Authencation, Authorition, Accouting
* Dùng port: 1812, Accouting dùng 1813.
* Giao thức UDP, chuẩn RFC 2865
* Giao thức hỗ trợ PAP, CHAP, MSCHAP, …



1. RADIUS OTP

* Xác thực cấp hai qua giao thức Radius.
* Hoạt động:

The device Radius Client Radius Server AD, LDAP

(NAS)

Enter user + pass

Response

Response

Send Otp

First authen

waiting

Enter Otp

Response

Response

Response

Check

Send user + pass

Gg authen

SMS

Access Reject/ Access Accept

Access Reject/ Access Accept

Access-Challenge

+ Từ chối truy cập - **Access Reject**: Người dùng bị từ chối truy cập vào tất cả các tài nguyên mạng.

+ Yêu cầu gửi thêm thông tin truy cập - **Access Challenge**: Yêu cầu thông tin bổ sung từ người dùng mã OTP.

+ Chấp nhận truy cập **- Access Accept**: Người dùng được cấp quyền truy cập.

* **Hoạt động:**
* Các loại xác thực:

+ Nhập user, pass -> sau đó mới nhập otp

+ Nhập user, pass, nhập luôn otp

+ Nhập user, pass nối chuỗi với otp.

Nhập user, pass -> sau đó mới nhập otp

+ User thực hiện đăng nhập với user, pass.

+ User, pass sẽ được gửi qua Radius Client, ở đây là NAS (Netword Access Server) máy chủ truy cập mạng. NAS được tích hợp Radius.

+ NAS gửi user, pass cho Radius Server.

+ Radius Server check user, pass qua AD (LDAP, CD).

+ Sau đó gửi lại thông báo cho NAS.

+ Nếu xác thực thành công thì Radius Server gửi Access Challenge cho NAS.

+ Radius Client sẽ gửi lại cho User để yêu cầu nhập mã OTP.

+ User truy cập bên thứ 3 lấy mã otp và nhập mã, gửi qua NAS

+ NAS gửi qua bên Radius server để check và gửi lại phản hồi.

+ Nếu thành công người dùng được phép truy cập.

Nhập user, pass, nhập luôn otp

+ User truy cập bên thứ 3 lấy mã otp

+ User thực hiện đăng nhập với user, pass, nhập mã OTP

+ User, pass sẽ được gửi qua Radius Client, ở đây là NAS (Netword Access Server) máy chủ truy cập mạng. NAS được tích hợp Radius.

+ NAS gửi user, pass cho Radius Server.

+ Radius Server check user, pass qua AD (LDAP, CD).

+ Nếu xác thực thành công thì Radius Server sẽ check mã Otp.

+ Sau đó gửi lại thông báo cho NAS. NAS gửi lại cho User.

+ Nếu thành công người dùng được phép truy cập.

Nhập user, pass nối chuỗi với otp.

+ User truy cập bên thứ 3 lấy mã otp

+ User thực hiện đăng nhập với user, pass, nhập mã OTP

+ User, pass sẽ được gửi qua Radius Client, ở đây là NAS (Netword Access Server) máy chủ truy cập mạng. NAS được tích hợp Radius.

+ NAS gửi user, pass cho Radius Server.

+ Radius Server tách chuỗi pass để lấy pass và otp, sau đó check user, pass qua AD (LDAP, CD).

+ Nếu xác thực thành công thì Radius Server sẽ check mã Otp.

+ Sau đó gửi lại thông báo cho NAS. NAS gửi lại cho User.

+ Nếu thành công người dùng được phép truy cập.

* Radius Server: Server Radius Free

+ Host

+ Port: default: 1812

+ Secret: key

* Mở rộng: login lần đầu lưu địa chỉ mac của thiết bị.

+ Đăng ký Radius Otp với gg authen:

Mã QR

Xác thực với Google Authencation

+ Ở thiết bị Android/Ios, thêm mã -> Quét mã.

* Với google authencation, cơ chế sinh mã sẽ cần một khóa bí mật, thời gian vào hiện tại và hàm mã hóa.
* Hàm mã hóa sử dụng HMAC-SHA1: thuật toán:  hmac = SHA1(secret + SHA1(secret + input))
* original\_secret = xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

secret = BASE32\_DECODE(TO\_UPPERCASE(REMOVE\_SPACES(original\_secret)))

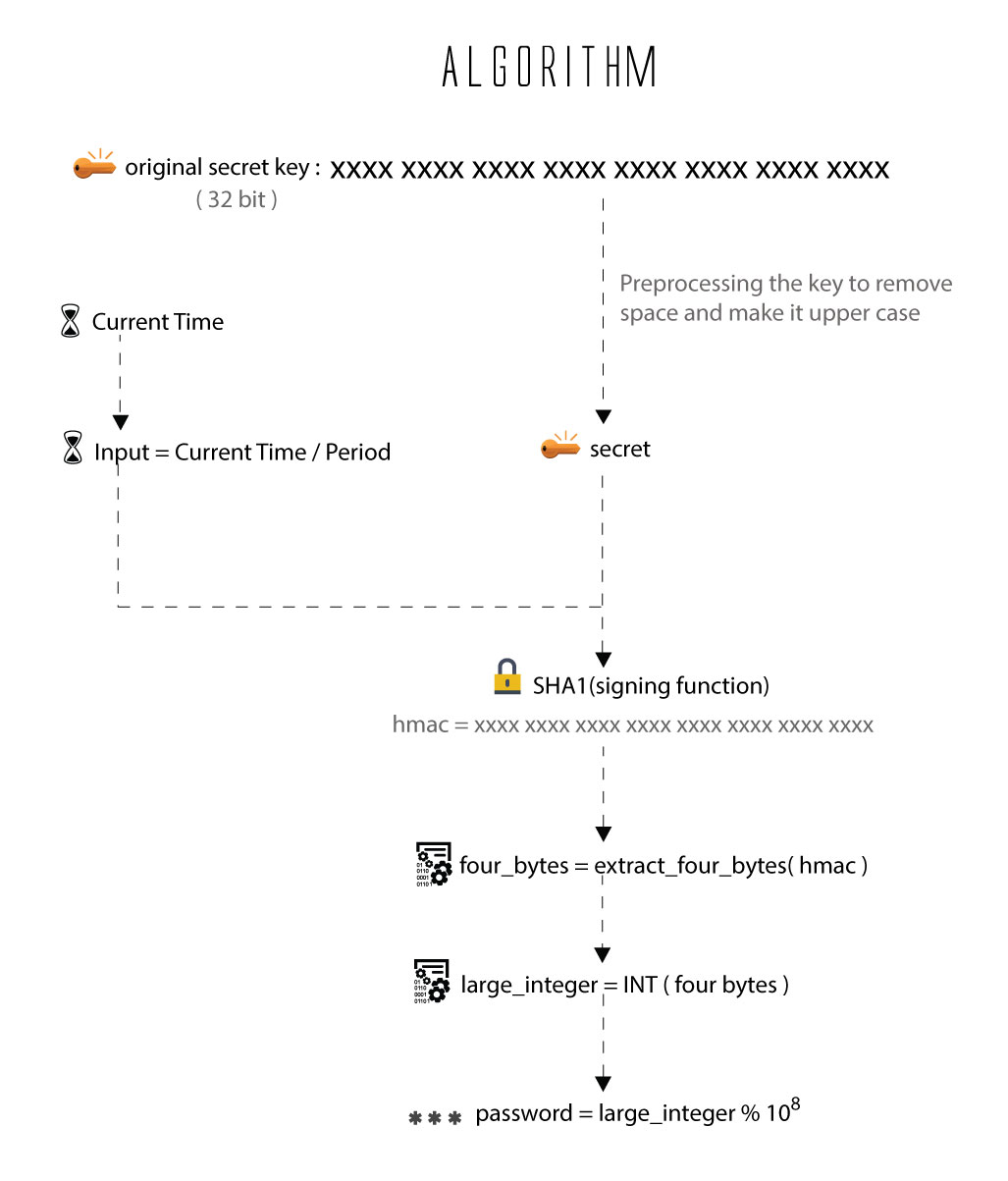
input = CURRENT\_UNIX\_TIME() / 30

hmac = SHA1(secret + SHA1(secret + input))

four\_bytes = hmac[LAST\_BYTE(hmac):LAST\_BYTE(hmac) + 4]

large\_integer = INT(four\_bytes)

small\_integer = large\_integer % 1,000,000



* *Mã QR sẽ được gen từ original\_secret, hoặc hiển thị bản rõ để có thể quét/nhập trên thiết bị.*
* Radius server sẽ xử lí hàm mã hóa để lấy được giá trị small\_integer và so sánh với input người dùng nhập vào. Key original\_secret được lưu ở radius server khi người dùng click vào bật gg authencation.

+ Đăng ký với SMS:

Xác thực với SMS

SĐT

* Khi người dùng bật xác thực Radius Otp với SMS thì số điện thoại người dùng sẽ lưu tại Radius Server.
* Sau khi login, Radius server sẽ random tạo ra mã Otp có thể lưu mã Otp này tại Cookie hoặc LocalStorage (được mã hóa) và có thời gian hết hạn là 30s-1p. Radius server xử lí hàm gửi mã Otp về SMS theo số điện thoại được lưu tại Radius Server của người dùng. Người dùng nhập mã, Radius Server so sánh với giá trị đã lưu tại Cookie hoặc LocalStorage rồi phản hồi cho Radius Client đưa lại cho người dùng.

+ Đăng ký với LoginTC:

* Đăng ký tài khoản LoginTC admin.
* Tạo domain, tạo Application.
* LoginTC kết nối với AD, LDAP.
* Radius Server kết nối LoginTc qua Application ID, Application API key.
* Tạo user (tên user cùng tên user trong AD).
* Tạo Issue Token, sinh ra 1 mã 10 kí tự, người dùng sẽ nhập mã này vào trong App LoginTC trên thiết bị. Lúc này server sẽ lưu lại tên thiết bị nhập mã 10 kí tự,
* Khi người dùng đăng nhập, LoginTC sẽ kiểm tra user, pass trong AD và chờ đợi phản hồi người dùng chấp nhận thông báo đẩy từ thiết bị, hoặc dùng mã Otp được sinh ra.
* Dùng Rest Api của LoginTC để gửi request: <https://cloud.logintc.com/api/>