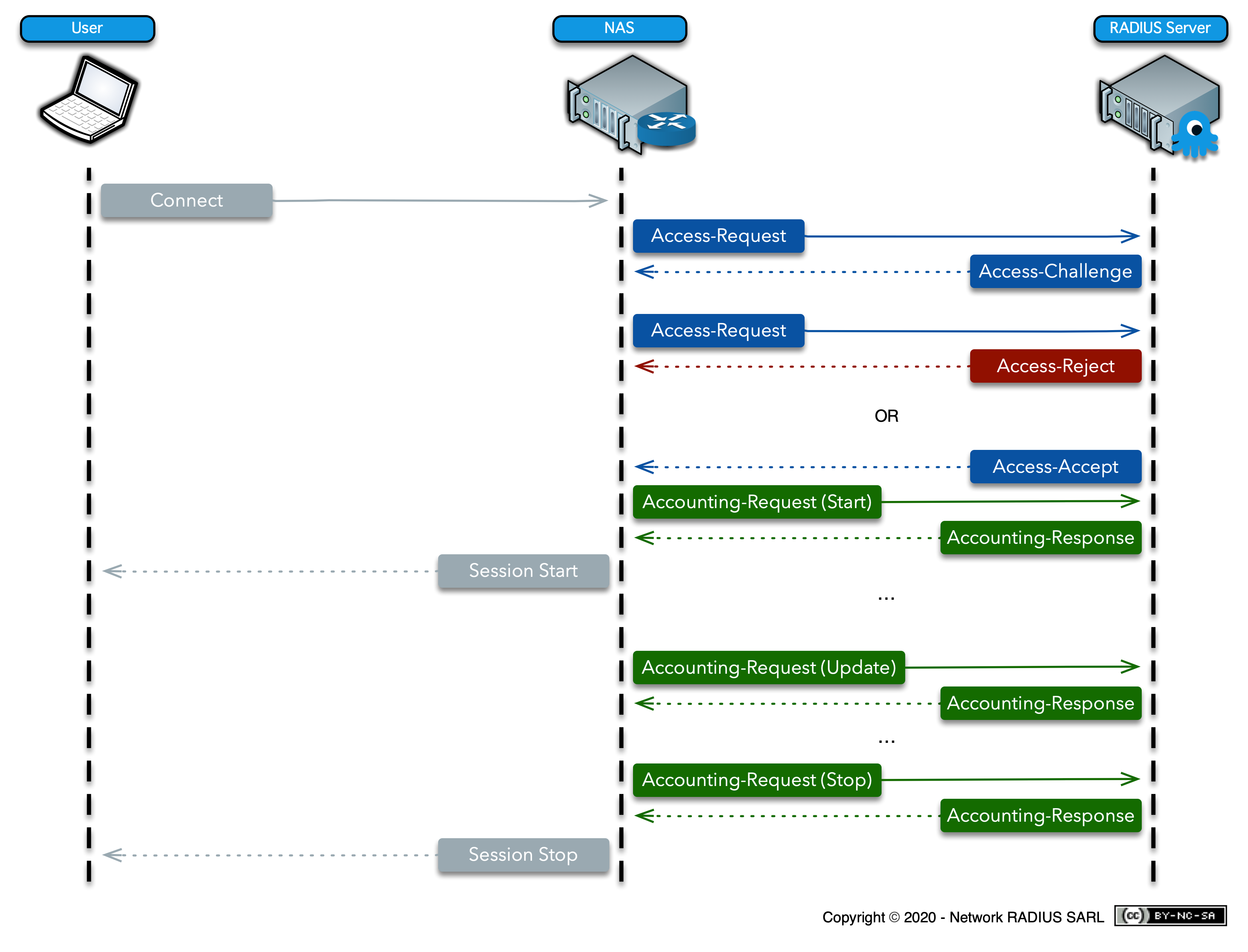
RADIUS OTP

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

Check in

Gg authen

Rsa securlId

LoginTC

SMS

Send Otp

First authen

waiting

Enter Otp

Response

Response

Response

Check

Send user + pass

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. Khi người dùng được xác thực, máy chủ RADIUS sẽ thường kiểm tra xem người dùng có được phép sử dụng dịch vụ mạng được yêu cầu hay không. Chẳng hạn một người dùng nào đó có thể được phép sử dụng mạng không dây, nhưng không được sử dụng VPN của công ty. Thông tin này có thể được lưu trữ cục bộ trên máy chủ RADIUS hoặc có thể được truy vấn tại một nguồn bên ngoài như LDAP hoặc Active Directory.

* Hoạt động:

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

+ Sau đó gửi lại thông báo cho client.

+ Nếu xác thực thành công thì Radius Server sẽ chờ đợi mã Otp. (mã otp từ bên thứ 3).

+ 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.

* 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.

* 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.