

Radius

I) Introduction :

Le protocole radius est conçu pour gérer les connexions d'utilisateurs à des services distants (autorisations, droit d'accès, tracabilité).

Le processus d'authentification est crypté, la vérification se base sur un annuaire LDAP ou base de données.

Diameter concurrence le radius. Diameter utilise le protocole TCP au lieu d'UDP dans le cas du radius.

II) Fonctionnement :

L'utilisateur se connecte à un client radius qui peut être une passerelle (proxy ou proxy reverse) ou un serveur radius.

Le client radius filtre les connexions en demandant à l'utilisateur ses identifiants de connexion afin de les communiquer au serveur radius. La communication entre le client et le serveur radius est sécurisée.

Le serveur radius vérifie les identifiants grâce à une base de donnée ou un annuaire LDAP.

Selon la zone d'accès demandée, le serveur radius pourra exiger des informations supplémentaires.

Radius utilisent les protocoles d'authentification PAP, CHAP ou EAP. Le chiffrement est de type clé privée/clé publique.

Le protocole EAP est très utilisés pour les réseaux sans fils.