Radius

- Radius (Remote Authentication Dial-In User Service)
- Radius architecture
- Radius Example

Radius (Remote Authentication Dial-In User Service)

Introduction

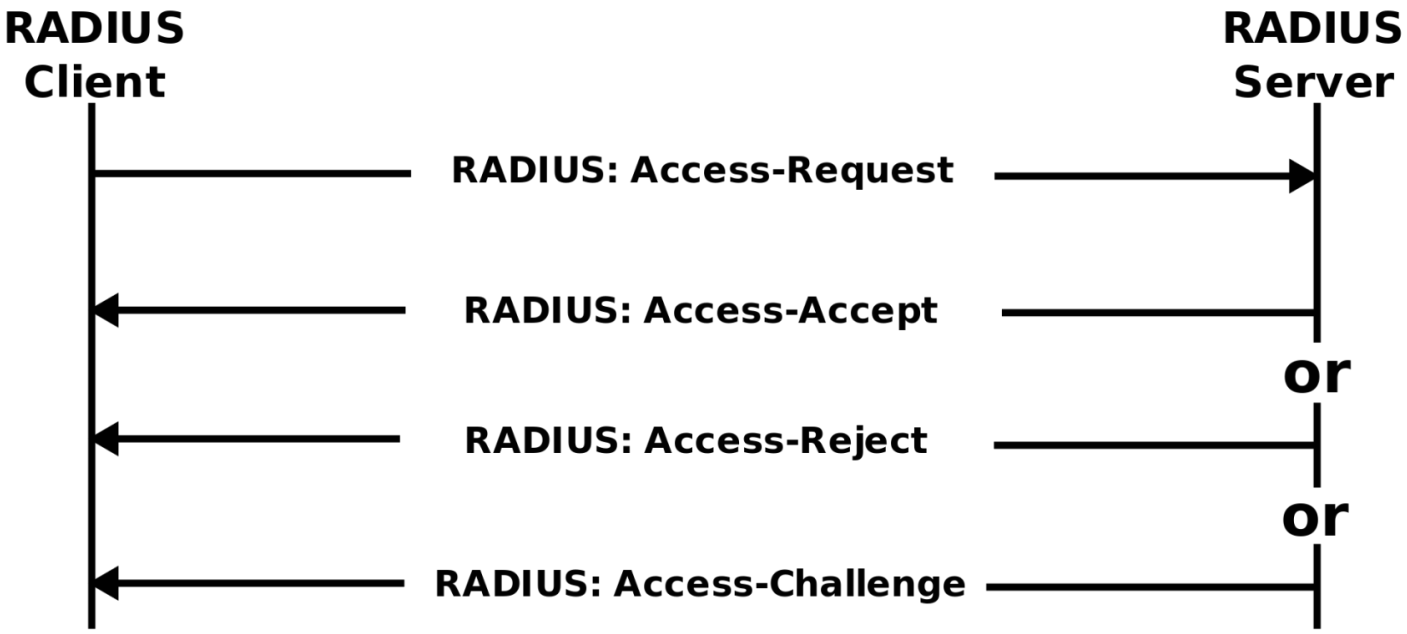
> The Radius protocol (Remote Authentication Dial-In User Service) is a networking protocol that authorizes and authenticates users who access a remote network.

---

https://es.wikipedia.org/wiki/RADIUS

Radius architecture

Introduction



Access Reject: The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.

Access Challenge: Requests additional information from the user such as a secondary password, PIN, token, or card. Access Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access Accept: The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server, or may be looked up in an external source such as LDAP or Active Directory.

---

https://en.wikipedia.org/wiki/RADIUS

Radius Example

Service Provider

