Radius information

November 13, 2013

1 Radius specifications

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for users that connect and use a network service.
Last version of the protocol normalized by the IETF in two RFCs (June 2000):

- `RFC2865` : RADIUS Authentication
- `RFC2866` : RADIUS Accounting

The RADIUS protocol uses UDP.

2 How does it work ?

2.1 Authentication and Authorization

UDP ports: 1645 or 1812
The authentication is initiated by a client that can be a NAS (Network Access Server), an wireless access point, a firewall, another server, etc. The RADIUS server manage this request and make a lookup, if necessary, in an extern database (SQL, LDAP,...).

The user or machine sends a request to a Remote Access Server (RAS) using user's access credentials. Those credentials are passed to the RAS device via the link-layer protocol. The RAS then sends an **Access Request** message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol (the request includes access credentials such as password and username).
The RADIUS server checks that the information is correct and sends back one of the three following responses :

- `Access Reject` : The user cannot access to the requested network resources. The reasons may include a failure to provide proof of identification or an unknown or inactive user account.
- `Access Challenge` : The RADIUS server asks for more information (the client will respons with another Access-Request packet). The 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 RAS.

- `Access Accept` : The user is granted access.

The RADIUS identification can be enhanced with a **autorization** like the user's IP address, his maximal connection time, QoS parameters,...

2.2 Accounting

UDP ports: 1646 or 1813
The accounting uses 2 packets :

- `Accounting Start` : It's simply a **Accounting-Request** packet with a `acct_status_type` attribute with the value **start**. This packet is sent to the RADIUS server after the authentication and contains some data (username, IP address, connection date & hour,...).
- `Accounting Stop` : Same type of packet but here the `acct_status_type` attribute value is **stop**. When the user quits the service or when the RADIUS deconnects him because of inactivity this packet is sent (either from the user or the server). There are generally a lot of data in this packet (connection duration, number of packets exchanged, information on websites visited, etc.).

There is also a special record called the `Interim Update`. It is sent by the NAS or the RADIUS server to update the status of the current connection.

3 Password protocols

Natively, 2 protocols :

- `PAP` : Password Authentication Protocol. Exchange in the **clear**.
- `CHAP` : Challenge Handshake Authentication Protocol. It works 3 steps :
  - After the authentication, the RADIUS server sends a *challenge* to the user. It is a 255 octets value randomly generated.
  - The user responds with a value computed with the challenge and his password using a hash function like MD5 (appends the password and the value and then hashes that result). He sends back to the RADIUS server the value.
  - The server realize the same operation and compares its results with the value received. It then accepts or refuses the connection.

  CHAP sends after a fixed amount of time a new challenge to the user.
- `EAP` : Extensible Authentication Protocol.
- `802.1X`

Now we have the Microsoft variations:

- `MS-CHAP` : RFC2433
- `MS-CHAP-V2` : RFC2759

4 Current Case

Two RADIUS servers at UCL and three LDAP servers.

- `Radius1` : radius1.sri.ucl.ac.be (130.104.1.9)
  - `PRS` : Personnel (port 1822) — Dossier *radiusLDAP1*
  - `ETD` : Etudiants (port 1832) — Dossier *radiusLDAP2*
  - `GUEST` : Guests (port 1852) — Dossier *radiusLDAP4*
  - `EDUROAM` : Eduroam (port 1812) — Dossier *radius*
- `Radius2` : radius2.sri.ucl.ac.be (130.104.1.8)
  - `PRS` : Personnel (port 1822) — Dossier *radiusLDAP1*
  - `ETD` : Etudiants (port 1832) — Dossier *radiusLDAP2*
  - `GUEST` : Guests (port 1852) — Dossier *radiusLDAP4*
  - `EDUROAM` : Eduroam (port 1812) — Dossier *radius*

About the LDAP servers :

- `LDAP ANNUAIRE` : Adresses mails UCL
- `LDAP OASIS` : Active directory
- `LDAP ID GLOBAL` : Users information (+SSL)