Network System

Radius Protocol

Claude Duvallet

University of Le Havre
Faculty of Sciences and Technology
25 rue Philippe Lebon - BP 540
76058 Le Havre Cedex, FRANCE
Claude.Duvallet@gmail.com
http://litis.univ-lehavre.fr/∼duvallet/index-en.php

Outline

1. Introduction
2. Functioning of the protocol Radius
3. WPA protocol
4. 802.1x protocol
5. EAP protocol

Bibliography

- **Serge Bordères.** *Authentification réseau avec Radius: 802.1x, EAP, FreeRadius.* Eyrolles. 2006.
- **Jonathan Hassell.** *Radius.* O'Reilly. 2002.

General principles about Radius server

- Authentication protocol, firstly created by Livingston.
- Define inside the RFC 2865 and 2866.
- It works like a client/server system which is in charge of the creation of the distant users access to the network.
- Main protocol used by the internet provider:
  - relatively standard,
  - offering some functionality of compatibility which allow the Internet provider to bill precisely their clients.
- RADIUS protocol allow to do a link between the identification need and a database of users by carrying out the transport of the authentication data in normalized way.

Principle of the functioning of the protocol Radius

- RADIUS mainly use:
  - a server (the RADIUS server), linked to an identification base (database, LDAP, etc.),
  - a RADIUS client, called NAS (Network Access Server), which is an intermediary between the final user and the server.
- All the transactions between the RADIUS client and the RADIUS server is crypted.
- The RADIUS server can also be used a proxy server, that is to say to transmit the request from the client to other RADIUS server.
- The server answer to the requests for authentication by using an outside base if necessary: SQL database, LDAP, users account of a host o a domain.
  - a RADIUS server have for this many interfaces or methods.

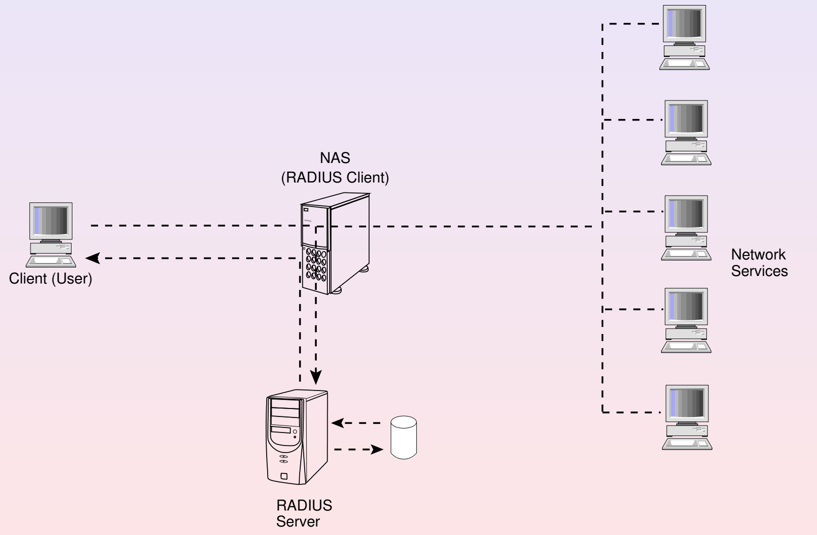
Functioning scenario (1/2)

- A user send a request to the NAS in order to authorize a distant connection.
- The NAS send the request to the RADIUS server.
- The RADIUS server look in its database of identification in order to know the scenario of identification requested by the user.
- Either the current scenario can be use, either an other method of identification is asked to the user. The RADIUS server return one of the four following answers:
  - **ACCEPT**: the identification has succeeded.
  - **REJECT**: the identification has failed.
  - **CHALLENGE**: the RADIUS server wish to have more information from the user and give a challenge.

Functioning scenario (2/2)

- An other answer is possible: **CHANGE PASSWORD** where the RADIUS server asks the user for a new password.
- Change-password is an VSA attribute (Vendor-Specific Attributes), that is to say it is specific to a provider.
- After this phase of authentication, a phase of authorization is beginning, where the server is sending the authorization to the user.

Diagram of the functioning of the RADIUS protocol



Password protocols

- At the beginning, RADIUS know two protocols of password:
  - PAP (exchange in clear of the name and the password,
  - CHAP (exchange based on a hashing from two part with only an exchange of the challenge).
- The protocol has two separate attribute: User-Password and CHAP-Password.
- Since, Microsoft has created two new protocols based on the first one: MS-CHAP and MS-CHAP-V2.
- Their similarity with CHAP allow them to be transported with RADIUS by the same way thank to the server only if it is possible to transport them end-to-end from the supplicant to the RADIUS client, from the client to the RADIUS server and finally from the RADIUS server to the database of identification.

Limitations of RADIUS protocol (1/3)

- RADIUS has been designed for identification by modem, so for slow links with a little security:
  - that's why UDP protocol has been chosen.
  - this technical choice for a non aggressive protocol leads to difficult exchanges based on procrastination and exchange of acknowledgements.
  - ⇒ Diameter (which should replace RADIUS) use TCP or STCP.
- RADIUS has an identification based on the principle of the couple name/password:
  - perfectly adapted when it has been created (1996),
  - this notion has had to be adapted
    Example: for the identification of mobile phone by the IMEI number or the call number (Calling-Station-ID in Radius) without a password (whereas the RFC fordid the empty password!).

Limitations of RADIUS protocol (2/3)

- RADIUS make a clear transport, only the password is crypted by hashing:
  - the only security is based on the only shared secret and so the exchanges between the client and the server must be secured by a Virtual Private Network (VPN) for example,
  - ⇒ Diameter may use IPSec or TLS.
- RADIUS limits the attributes:
  - they are managed as a "Pascal" string with a byte in head that give the length within 255 bytes, which is coherent with the notion of login/password,
  - but not adapted for an in introduction of biometry (eye, fingerprint), of cryptography (certificate),
  - ⇒ Diameter use attributes with 4 bytes elsewhere 1 bytes (it is already present in some extensions EAP of RADIUS like TTLS).

Limitations of RADIUS protocol (3/3)

- RADIUS est strictly client/server:
  - that's why there are many problems with the owner protocols when a server must kill a hacker session on a client,
  - ⇒ Diameter has got some mechanisms to call the client from the server.
- RADIUS has not any mechanisms for the identification:
  - if you take the role of server it may be a good way to take the names and the passwords,
  - ⇒ EAP work with a mutual identification the client and the server.

WPA protocol (1/2)

- Objective: improvement of the WEP protocol which have some weakness
  - WEP use simple algorithms which can be easily broken.
  - It isn't possible to authenticate a computer or a user who will connect to the network thanks to the WEP protocol.
- Definition of two new methods of crypting and integrity control:
  - TKIP (Temporal Key Integrity Protocol):
    - better adapted to the existing material,
    - use RC4 as algorithm to crypt,
    - add an integrity control MIC,
    - introduce a mechanism to manage the key (dynamic creation of keys at regular interval of time).
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):
    - more efficient than TKIP,
    - use AES as algorithm to crypt,
    - completely not compatible with current material ⇒ a solution at a long term.

WPA protocol (2/2)

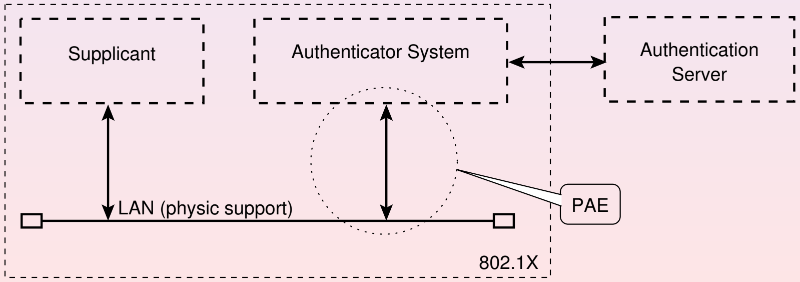
- WPA use the 802.1X protocol .
- Other name: EAP Over LAN (EAPOL).
- It allows to authenticate the computers or the users connected to the network.
- It allows to transfer some packets of authentication to different element of the network.
- It provides a mechanism to exchange keys which will be used to crypt the communications and control the integrity.
- WPA-PSK (Pre Shared Key) allow private individual to benefit from WPA without having an authenticate server:
  - at the beginning: we use a static key or a passphrase (like for WEP),
  - but also use TKIP,
  - then: automatically change the key at regular interval of time.

802.1x protocol

- IEEE 802.1X is a standard from IEEE for the network access control based on the ports.
- It is a part of the group of protocol IEEE 802 (802.1).
- This standard provide an authentication to the equipments connected at an Ethernet port.
- It is also use by some WiFi access point, and it is based on EAP.
- 802.1X is a functionality available on some network router.

Actors of 802.1x

- **Supplicant:** it represents the system to identify (the client/user).
- **Port Access Entity (PAE):** it represents the access point to the network.
- **Authenticator System:** it is the system which is in charge of the authentication. It controls the ressources available thanks to the PAE.



Supplicant

Authenticator System

Authentication Server

LAN (physic support)

PAE

802.1X

Authentication

- Authenticator system has a behavior similar to a proxy between the supplicant and the authenticator server.
- If the authentication succeed, the authenticator system give the access to the ressource it controls.
- The authenticator server manage the authentication by talking with the supplicant according the authentification protocol used.
- In most of the implementation of the 802.1X protocol, the authenticator system is a network equipment (Ethernet router, wireless access point, or IP router).
- The supplicant is a computer or a host.
- The authenticator server is typically a RADIUS server or any other equipment which is able to make authentication.

Port Access Entity (PAE)

- The main new thing in 802.1X consist of to divide the physical access port into two logical access port connected which are connected in parallel on the physical port.
- The first logical access port is said “to be controlled” and may have two state: «open» or «close».
- The second logical access port is always available but it only manage the specific message of the 802.1X protocol.
- This model do not take into account the physical aspect of the connection. It may be:
  - a RJ45 plug (case of the copper transmission).
  - SC or MT-RJ connector (in case of optic fiber).
  - a logical access to the network (case of the wireless access 802.11{a,b,g}).

EAP protocol

- EAP (Extensible Authentication Protocol) is a protocol designed to extend the functions of the RADIUS protocol for some kind of identifications more complex.
- It is independent from the material of the RADIUS client is directly negotiated with the supplicant.
- That’s why it has been possible to install on a great number of network equipment:
  - it only use two RADIUS attributes which are used as a transport protocol,
  - it has lead to the creation of a great number of different type of EAP: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MS-CHAP-V2, EAP-AKA, EAP-LEAP and EAP-FAST (Cisco), EAP-SIM, etc.

EAP-MD5

- It is the more simple protocol.
- The client is authenticated by the server thanks to a mechanism of challenge and answer:
  - The server send a random value (the challenge).
  - The client concat to this challenge the password and compute, thanks to MD5 algorithm, an encrypted value that it send to the server.
  - The server that know the password compute its own encrypted value and compare the two values. According to the result of the comparison, it decides to validate or not the authentication.
- A listening of the network traffic, in the case a password too much simple, may allow to find the password thanks to an attack based on dictionnary.

LEAP

- It is the own method of CISCO.
- It is based on the used of shared secret to mutually authenticate the server and the client.
- It does not use any certificate.
- It is based on the exchange of challenges and answers.

EAP-TTLS

- EAP-TTLS (tunneled Transport Secure Layer).
- It uses TLS as a tunnel to exchanges some couples of attributes for the authentication.
- Practically, any methods of authentication can be used.

PEAP (Protected EAP)

- It is a methods similar in its objectives its realization to EAP-TTLS.
- It has been developed by Microsoft.
- It uses a TLS tunnel to circulate EAP.
- So, we can use all the authentication methods supported by EAP.

EAP-TLS

- EAP-TLS: Extensible Authentication Protocol-Transport Layer Security
- It is the more efficient.
- The server and the client have their own certificate which will be used to a mutually authentication.
- It is relatively constraining because of the necessary to deploy a framework of keys management.
- TLS, the normalized version of SSL (Secure Socket Layer), is a secure transport (encryption, mutual authentication, integrity control).
- It is used by HTTPS, the secure version of HTTP and to secure the Web.