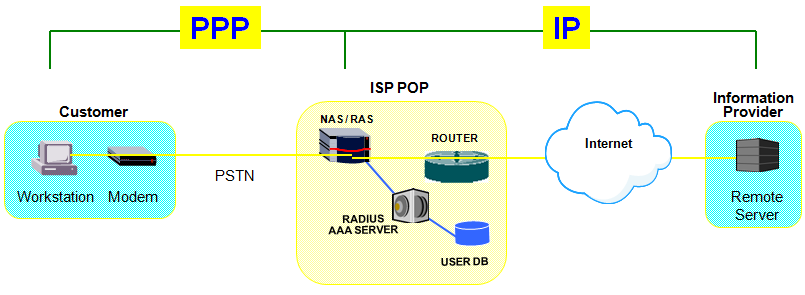
**RADIUS**

**Remote Authentication Dial-In User Service**

È un [protocollo AAA](http://it.wikipedia.org/wiki/Protocollo_AAA) (authentication, authorization, accounting) utilizzato in applicazioni di accesso alle reti o di mobilità [IP](http://it.wikipedia.org/wiki/Internet_Protocol). RADIUS è attualmente lo standard de-facto per l’autenticazione remota, prevalendo sia nei sistemi nuovi che in quelli già esistenti.

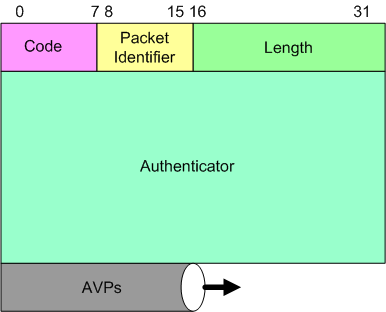


L'utente o macchina invia una richiesta ad un Network Access Server (NAS) di accedere ad una particolare risorsa di rete utilizzando le credenziali di accesso. Il NAS RADIUS invia un messaggio al server RADIUS con la richiesta di autorizzazione a concedere l'accesso,tale richiesta include le credenziali di accesso, di solito in forma di nome utente e password o altri certificati di sicurezza fornite dagli utenti. Inoltre, la richiesta può contenere altre informazioni che la NAS conosce l'utente.

Il server RADIUS verifica che le informazioni siano corrette utilizzando sistemi come l'autenticazione EAP (Extensible Authentication Protocol)

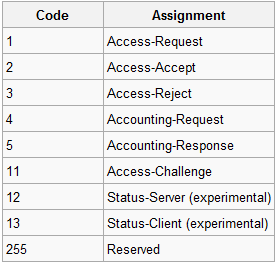
Il server può fare riferimento a fonti esterne - comunemente SQL, Kerberos, LDAP, Active Directory o server - per verificare che le credenziali dell'utente.

* STRUTTURA PACCHETTO:

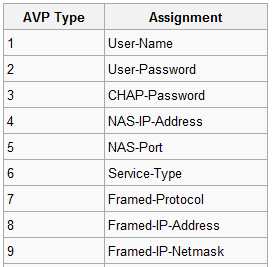


I campi sono trasmessi da sinistra a destra, a cominciare con il codice, l'identificazione, la lunghezza, l'autenticatore e gli attributi.

* I **codici** (decimali) sono assegnati come segue:



* Il campo **Identifier** è utilizzato per effettuare il matching durante le richieste e le risposte
* Il campo **Length** indica la lunghezza dell’intero pacchetto
* L’**Authenticator** è utilizzato per autenticare la risposta da parte del server RADIUS ed è qui che viene crittografata la password
* **Attribute Value Pairs** (avps): attributi utilizzati in entrambi i dati della richiesta e della risposta per le operazioni di authentication, authorization ed accounting



* FUNZIONAMENTO

**Authentication ed Authorization**

L’intero processo ha inizio quando un client crea un pacchetto RADIUS Access-Request, includendo almeno gli attributi User-Name e User-Password, e generando il contenuto del campo identificatore.

Il processo di generazione del campo identificatore non è specificato nel protocollo RADIUS, ma è solitamente implementato come un semplice contatore incrementato ad ogni richiesta.

Il campo authenticator contiene una Request-Authenticator, ovvero una stringa di 16 byte scelta in modo casuale. L'intero pacchetto è trasmesso in chiaro, a parte per l’attributo User-Password, che è protetto nel modo seguente: il client e il server condividono una chiave segreta. Tale chiave viene unita con la Request Authenticator, e l'intera stringa viene sottoposta a una funzione hash MD5 per la creazione di un valore di 16 ottetti, sottoposto a sua volta a un XOR con la password immessa dall’utente (e se tale password è più lunga di 16 ottetti, vi è un calcolo MD5 addizionale, utilizzando il testo cifrato anziché la Request Authenticator).

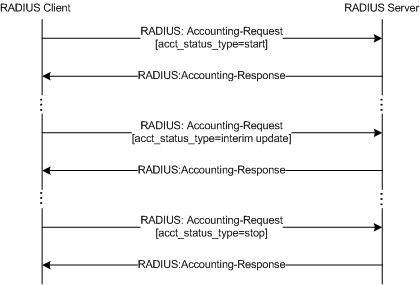
Il server riceve il pacchetto Access-Request e verifica di possedere la chiave segreta per il client. In caso negativo, il pacchetto viene silenziosamente ignorato. Poiché anche il server è in possesso del segreto condiviso, è possibile utilizzare una versione modificata del processo di protezione del client per ottenere la password in chiaro. Quindi il server consulta il database per convalidare username e password; se la password è valida, il server crea un pacchetto Access-Accept da rimandare al client. In caso contrario, crea un pacchetto Access-Reject e lo invia al client.

Entrambi i pacchetti Access-Accept e Access-Reject utilizzano lo stesso valore identificatore del pacchetto Access-Request del client, e hanno una Response Authenticator nel campo Authenticator. La Response Authenticator è la funzione hash MD5 del pacchetto di risposta con l’associata Request Authenticator, concatenata con il segreto condiviso.

Quando il client riceve un pacchetto di risposta, si accerta che esso combaci con una precedente richiesta utilizzando il campo identificatore. Se non esiste alcuna richiesta con lo stesso identificatore, la risposta è silenziosamente ignorata. Quindi il client verifica la Response Authenticator utilizzando lo stesso calcolo effettuato dal server, ed infine comparando il risultato con il campo Authenticator. Se la Response Authenticator non coincide, il pacchetto è silenziosamente ignorato.

Se il client riceve un pacchetto Access-Accept verificato, username e password sono considerati corretti, e l’utente è autenticato. Se invece riceve un pacchetto Access-Reject verificato, username e password sono scorretti, e di conseguenza l’utente non è autenticato.

**Accounting**

****

La misura e la documentazione delle risorse concesse ad un utente inizia quando gli viene concesso l'accesso alla rete da parte del NAS

* Acct\_status con il valore "Start" è inviato dal NAS al server RADIUS per segnalare l'inizio dell’accesso alla rete.
* "Start" di solito contiene anche le registrazioni di identificazione dell’utente e l’indirizzo di rete
* Periodicamente si ha un aggiornarmento sullo stato della sessione attiva.(Acct\_status=interim update) Il record tipicamente trasmette la durata della sessione corrente e le informazioni sui dati attuali di utilizzo.
* Infine, quando termina la connessione, viene inviato il record di stop e vengono fornite informazioni sugli utenti finali di utilizzo in termini di: tempo, pacchetti trasferiti, dati trasferiti e altre informazioni relative agli utenti della rete di accesso.