PROTOCOLLI PER LA SICUREZZA IN RETI WIRELESS

WPE, WPA, WPA 2

di Alessio Pastorino

Argomenti

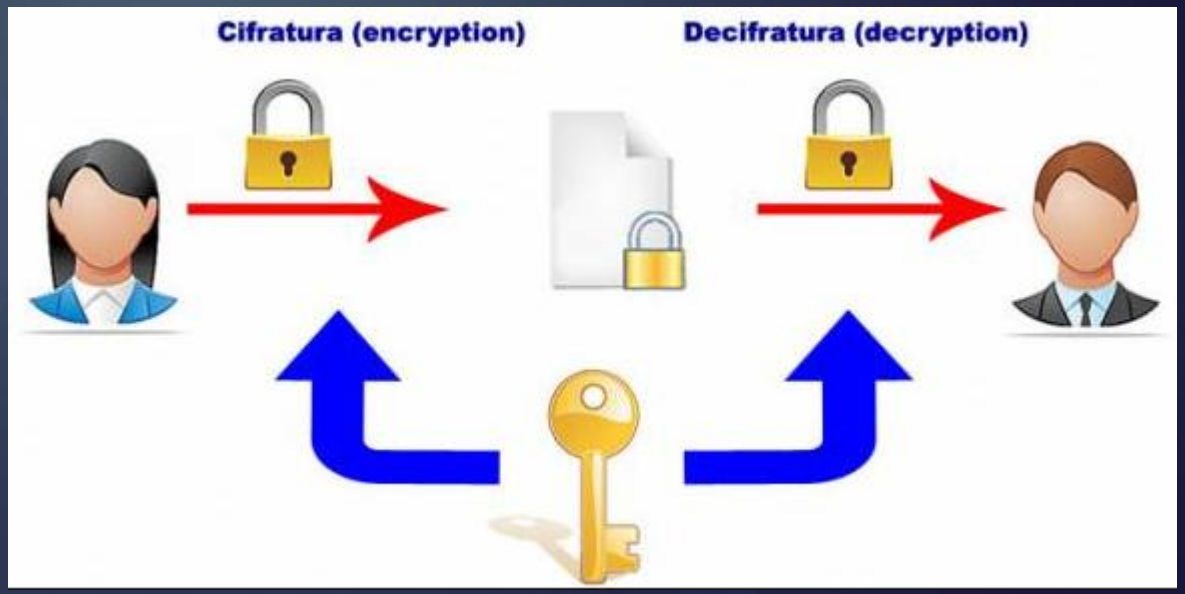
Introduzione

La crittografia(o cifratura) dal greco significa nascosto. E' una tecnica che viene utilizzata per realizzare reti sicure. Sicurezza informatica significa assicurare la ***riservatezza***, l'***autenticazione*** e il ***non ripudio*** delle informazioni archiviate o inviate attraverso reti di computer.

La crittografia ha lo scopo, di "offuscare" il messaggio, nascondendone il significato. Per rendere incomprensibile il contenuto di un messaggio, lo si altera attraverso un procedimento concordato tra il mittente e il destinatario.

Tale tecnica implica l'uso di una o più *chiavi*.

Ad esempio una *chiave* conosciuta da entrambi.



Tecniche di sicurezza nelle reti wireless

La maggior parte degli Access Point sono programmati per gestire tre tipologie di standard crittografici:

- Wired Equivalent Privacy ***WEP***
- Wi-Fi Protected Access ***WPA***
- Wi-Fi Protected Access2 ***WPA2***

Ora analizziamo nel dettaglio le tecniche elencate qui sopra

WEP

Il **Wired Equivalent Privacy** (*WEP*) è stato progettato per garantire un livello di sicurezza pari a quello delle reti cablate. Questo protocollo è considerato come il minimo indispensabile per impedire a un utente di accedere alla rete locale.

Il protocollo WEP è stato creato per rafforzare questi tre punti:

- ***Riservatezza*** prevenire le intercettazioni casuali, codificando con l'algoritmo **RC4** i pacchetti inviati.
- ***Access Control*** proteggere l'accesso non autorizzato alla rete wireless
- ***Data Integrity*** prevenire l'alterazione dei messaggi

WPA

Il **W**i-Fi **P**rotected **A**ccess (WPA) è stato creato per sostituire il precedente sistema di sicurezza, ormai conosciuto per le sue numerose falle.

WPA è un protocollo che garantisce:

- aumento della dimensione della chiave(128 bit)
- aumento del numero delle chiavi in uso
- include il protocollo TKIP (Temporal Key Integrity Protocol) , che crea un'unica chiave per ogni client servito e la genera una nuova chiave tutte le volte che viene inviato un pacchetto sulla rete
- include un sistema apposito, migliore, per verificare l'autenticità dei messaggi, incrementando la sicurezza della **WLAN**

WPA 2

Lo standard WPA2, migliore del WPA, rende le reti Wi-Fi ancora più sicure e garantisce un elevato livello di confidenzialità dei messaggi scambiati.

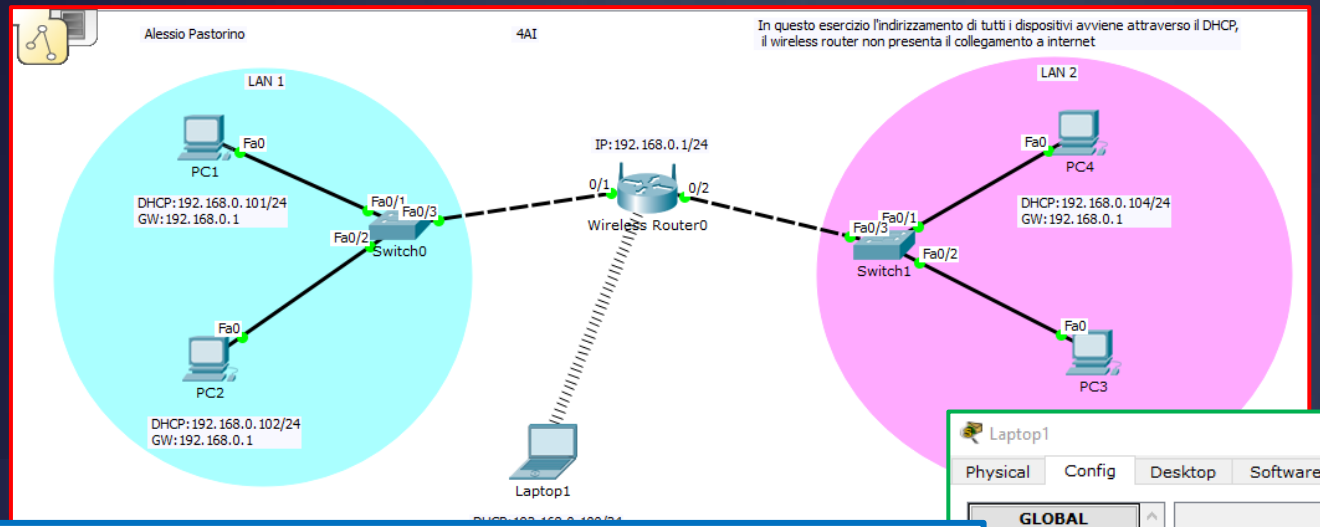
Nel WPA2 si è creata una scissione del processo di autenticazione dell'utente all'Access Point e il processo di cifratura dei messaggi scambiati tra sorgente e destinatario.

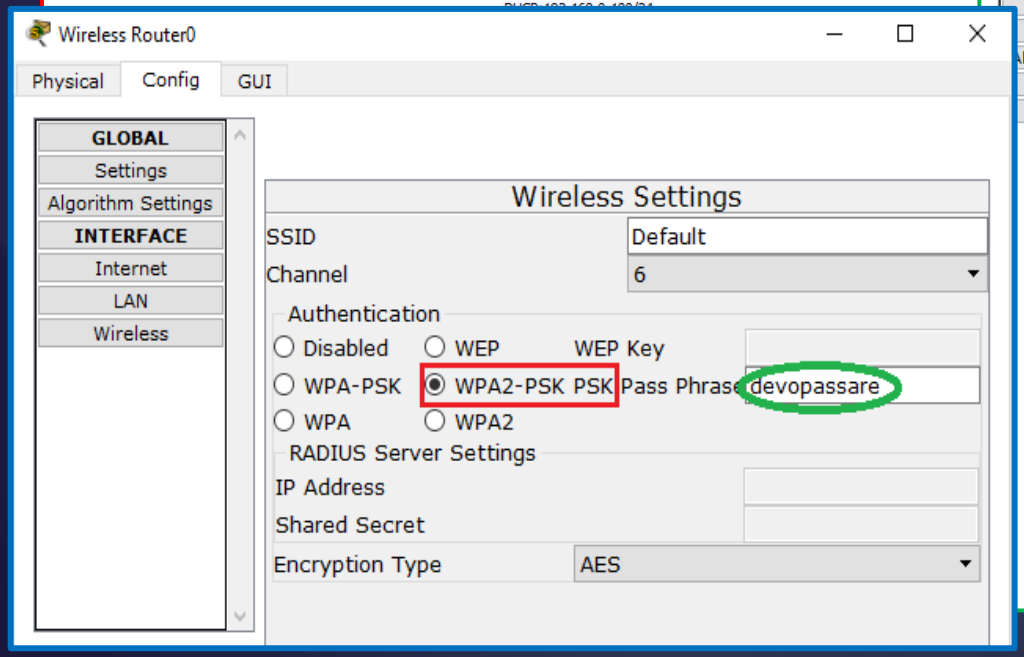
Nel WPA2 si utilizza una nuova architettura per le reti wireless detta **RSN** che usa, come processo di autenticazione, il protocollo 802.1X

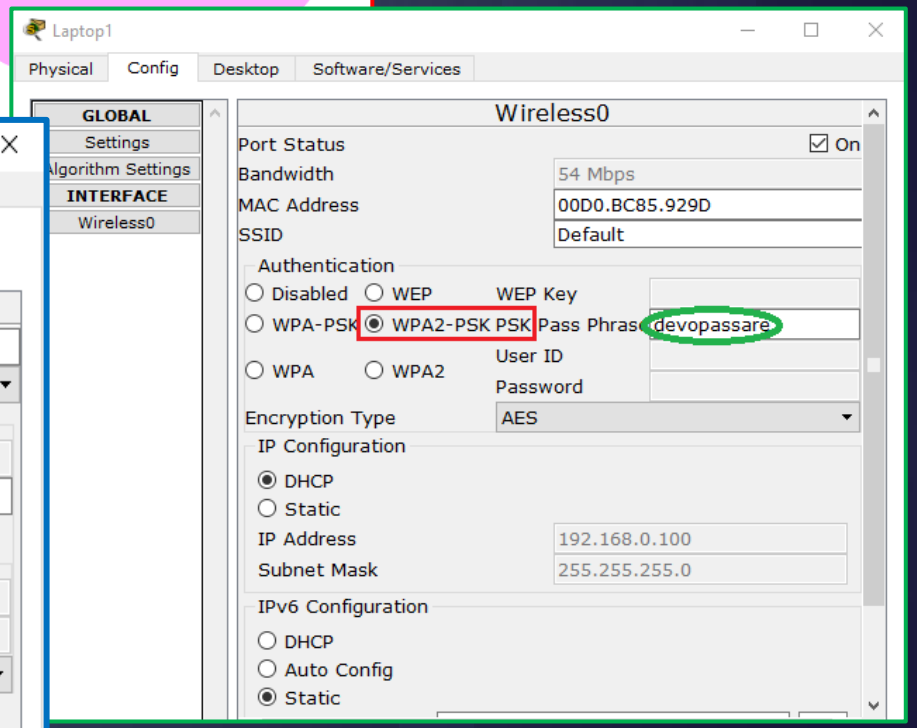
Questo protocollo è costituito da tre elementi:

- Il client richiede l'accesso alla rete
- L'Access Point (**autenticatore**) fornisce servizi alla rete e vigila gli accessi
- Il server di autenticazione ha il compito di gestire le **autorizzazioni**

Esempio in Packet Tracer







Glossario

Autenticazione: è il processo attraverso il quale viene verificata l'identità di un utente che vuole accedere ad un computer o ad una rete. [return]

Riservatezza (o confidenzialità): Si tratta di garantire che soltanto gli utenti autorizzati abbiano accesso alle informazioni protette. [return]

Non ripudio: garantisce che i partecipanti ad una transazione non possano negare di averla eseguita: il mittente di un messaggio non può negare di averlo spedito e chi lo riceve non può negare di averlo ricevuto. [return]

RC4: è uno degli algoritmi di cifratura di flusso più diffusi. [return]

RSN: è un protocollo che tiene traccia delle associazioni tra dispositivi connessi alla rete. [return]

WLAN: sono reti locali wireless che consentono l'accesso di un utente da qualunque posizione nell'area coperta della rete stessa. [return]

Sitografia

- http://math.unipa.it/~fbenanti/Crittografia291111.pptx
- http://www.mrwebmaster.it/reti/protocollo-wpa_10471.html
- http://www.mrwebmaster.it/reti/debolezze-wep_10470.html
- http://www.apav.it/sitostudenti/sito%20giur/federica/crit.htm
- http://www.mrwebmaster.it/reti/standard-802-11i-wpa2_10472.html

Spero di essere stato chiaro e sintetico nell'esporre i contenuti.

GRAZIE E ARRIVEDERCI !!