Access Point, Protocolli di Sicurezza e Hotspot

Access Point

L'**Access Point (AP), ha una normale connessione cablata Ethernet** 802.3 per uno switch, ma funge anche da base radio per il modulo **Wireless Terminal (WT).** Scopo dell'AP è trasformare trame Ethernet 802.3 in Trame Wirless 802.11 (più complesse)

I computer portatili hanno il modulo wireless WT integrato, mentre un personal computer desktop deve dotarsi di un modulo WT, per esempio realizzato attraverso una «chiavetta» USB.

Access Point

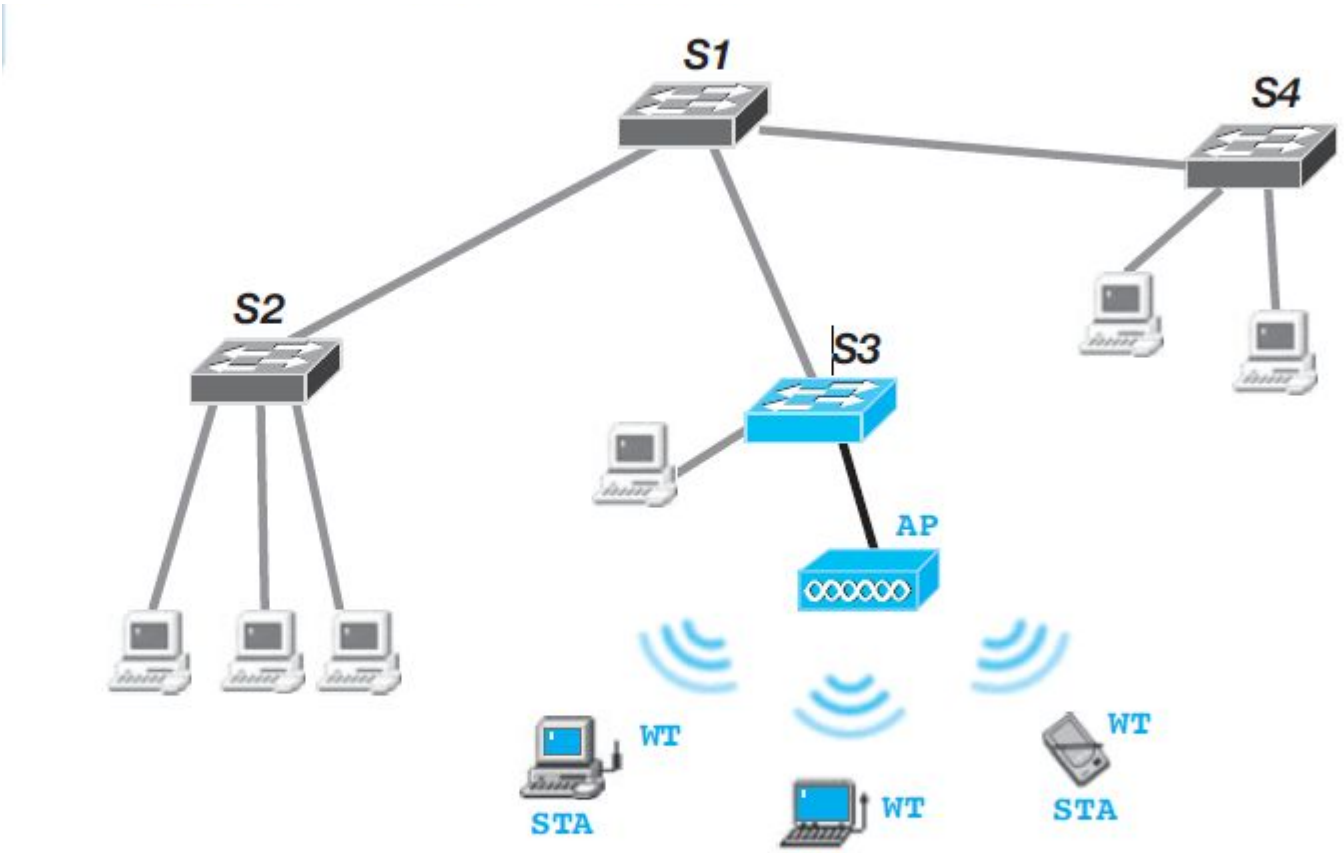
Il sistema dotato del modulo WT si comporta come un normale sistema connesso allo switch su cui l'Access Point relativo è connesso. Un Access Point può fornire l'accesso alla LAN ad una trentina di client WT differenti operanti nella sua cella radio. (Il numero di utenti varia in base ai tipi di AP.)

Access Point

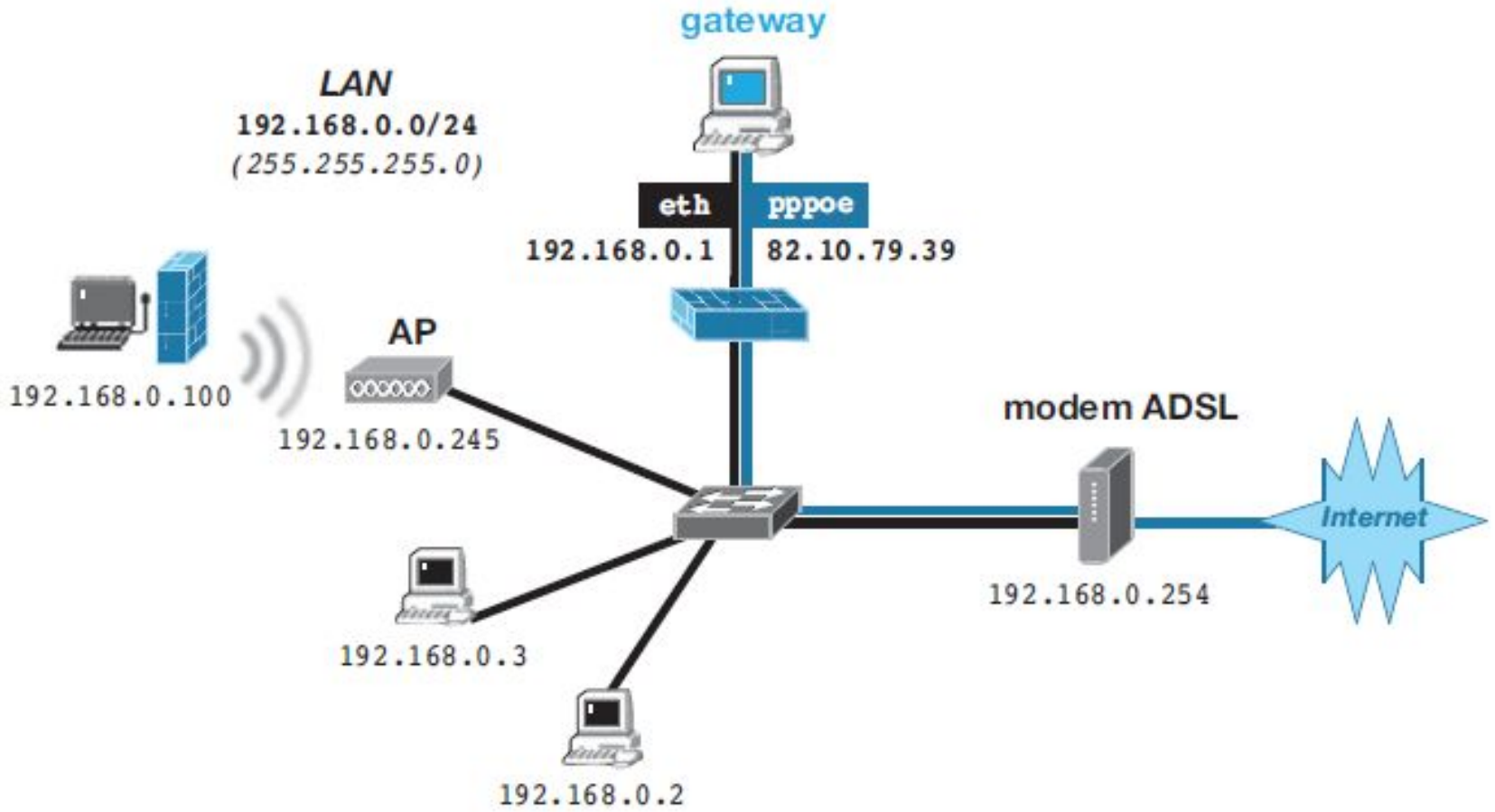
Siccome la comunicazione avviene tramite onde radio, essa può essere messa in crisi da particolari condizioni ambientali (per esempio, ostacoli come alberi, pilastri,muri di edifici), cosicché la portata dei dispositivi WiFi non sempre rispetta i valori promessi, che sono 30m per ambienti interni e 100m per ambienti esterni.

Ogni Access Point è riconoscibile tramite un nome sottoforma di stringa descrittiva (**SSID, *Service Set Identifier) in modo tale che un client possa*** consultare l'elenco dei SSID presenti nel suo raggio d'azione.

Esempio di architettura



Esempio di architettura



Comunicazioni Wirless

Accesso al canale

Sostanzialmente sono due le modalità di trasmissione wireless:

- **ad hoc**, o **IBSS** (Independent Basic Service Set): senza infrastruttura, è una connessione peer to peer utilizzata per sale conferenze, condivisione di periferiche, allineamento archivi ecc.;
- **infrastrutturata**, o **EES** (Extended Service Set): con un AP connesso alla rete cablata o a Internet, che richiede autenticazione e permessi di accesso, è utilizzata nelle reti aziendali, in uffi cio, in reti domestiche, in hotspot ecc.

Comunicazioni Wirless

Elusione delle collisioni

Per risolvere il problema di collisioni le WLAN utilizzano il protocollo ◂ livello MAC ▸ chiamato CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), cioè accesso multiplo con ascolto della portante ed elusione delle collisioni.

Dato che il client non si accorge delle collisioni, è il ricevente che deve gestire la comunicazione:

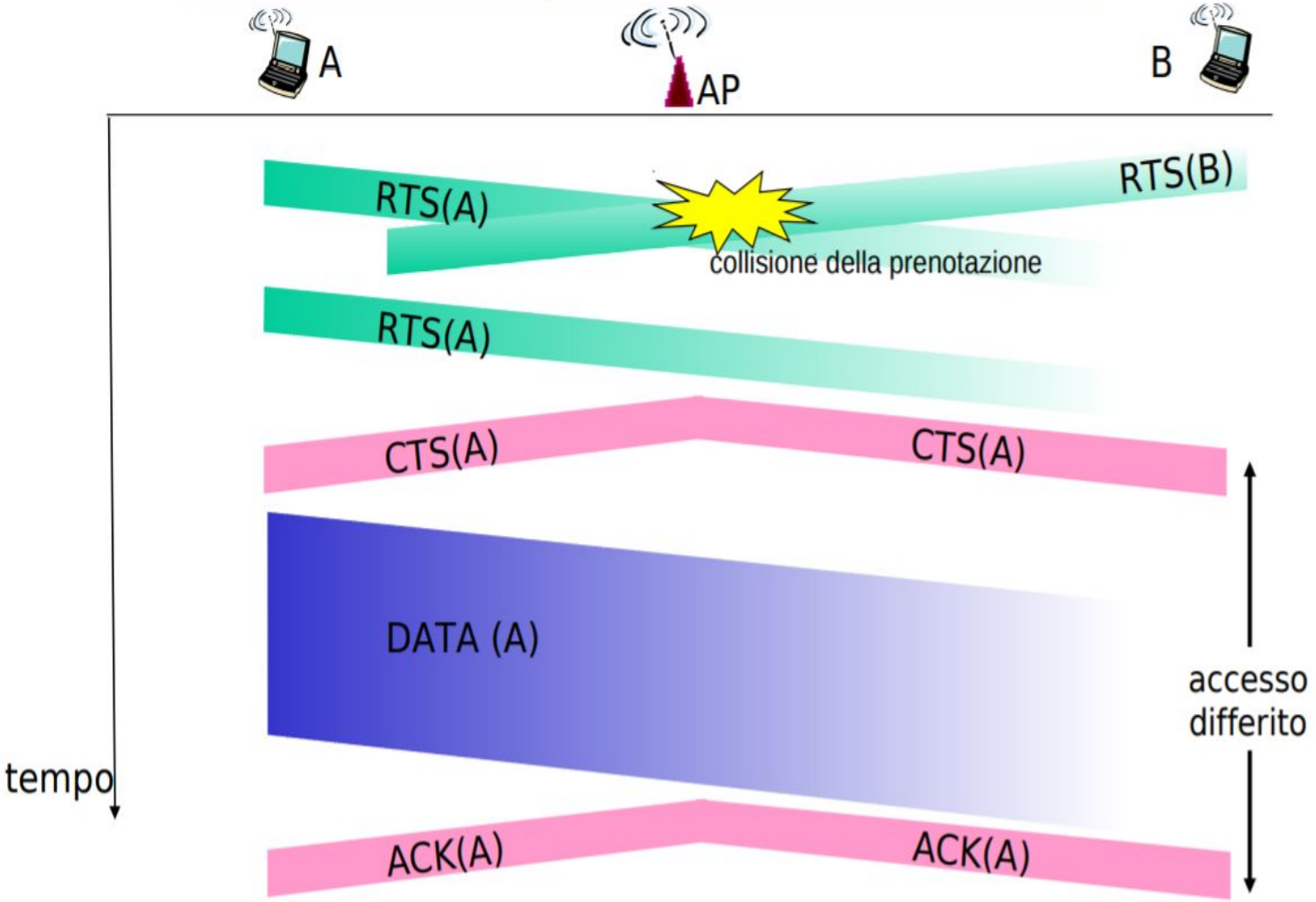
- il trasmettitore quando trova un canale libero invia un pacchetto di dati;
- il ricevente invia un segnale di conferma ricezione ACK;
- il trasmittente, se non riceve l'OK dal ricevente, considera il pacchetto perso e ripete la trasmissione.

Comunicazioni Wirless

La ***collisione*** avviene quando due emittenti sentono che un canale è libero e iniziano contemporaneamente a trasmettere; per eludere le collisione si utilizza il CA:

- il mittente inizia la comunicazione trasmettendo un pacchetto molto corto ***RTS*** (Request To Send);
- il destinatario risponde con un pacchetto ***CTS*** (Clear To Send);
- le altre emittenti prima di trasmettere si mettono in ascolto (carrier sensing), ricevono questi pacchetti e li interpretano come segnali di canale occupato e quindi evitano di trasmettere in intervalli successivi di tempo.

Evitare le collisioni: scambio di pacchetti RTS-CTS



Pacchetto 802.11: indirizzamento

Indirizzo 1: indirizzo MAC dell'host wireless o AP che deve ricevere il pacchetto

Indirizzo 2: indirizzo MAC dell'host wireless o AP che trasmette il pacchetto

Indirizzo 3: indirizzo MAC dell'interfaccia router cui l'AP è collegato

Indirizzo 4: usato solo in modalità ad hoc

Comunicazioni Wirless

Dato che gli indirizzi MAC delle schede Wi-Fi sono unici, come tutti gli indirizzi delle schede Ethernet, è possibile pensare di inserire una tabella di indirizzi autorizzati all'interno degli AP in modo che questi possano accettare solo i pacchetti trasmessi da indirizzi conosciuti. Questa soluzione non sempre è efficace in quanto per un malintenzionato è possibile "mascherare" da software l'indirizzo MAC camuffandolo e sostituendolo con indirizzi autorizzati.

Le specifiche 802.11 introducono il WEP (Wired Equivalent Privacy) per proteggere la rete e impedire che utenti non autorizzati ascoltino o immettano traffico sulla rete.

Comunicazioni Wirless

Si definisce **WEP** un frame così costituito:

|Frame Header | IV (24bit)|KeyID(2bit) | Dati Criptati(RC4)|

- il **WEP header** contiene 24 bit chiamati di **I**nitialization **V**ector (**IV**) e 2 bit di **KeyID**: vengono utilizzati per la determinazione della chiave **RC4** di 40 bit (***WEP key***) tra le quattro definite;
- i dati, criptati con la chiave RC4;
- un gruppo di 32 bit di parità (c(M)).

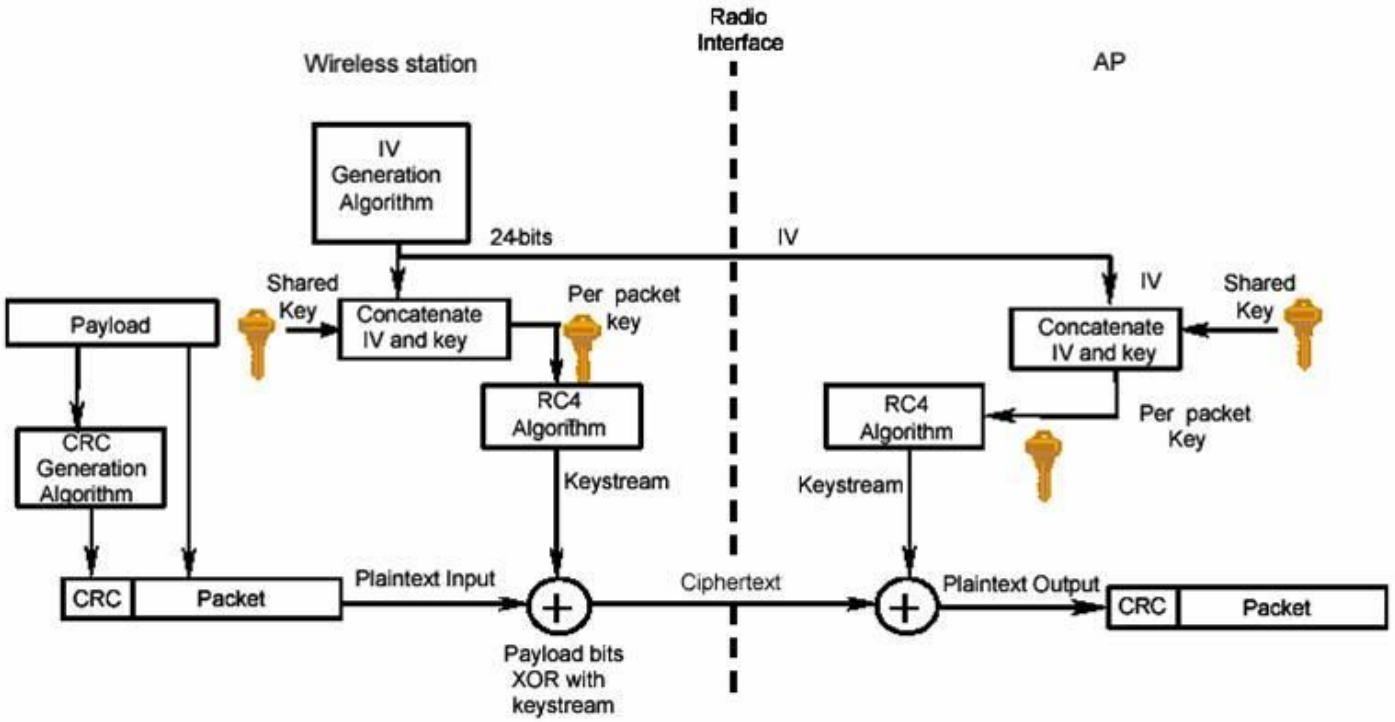
Il Key ID si riferisce a 4 chiavi possibili, trasmesse in chiaro quindi vulnerabili!!

(vedi Volume 1 Reti Wirless)

Accesso protetto

WEP (Wired Equivalent Privacy) IEEE 802.11

- *Algoritmo crittografico (key simmetrica) RC4*
- *Sistema di controllo dell'integrità dei dati CRC-32*



Accesso protetto

Per sopperire all'insicurezza del WEP, nel 2004 nasce il ***W****irless* ***P****rotected* ***A****cces*. (da 40 a 128 bit)

I metodi di protezione più comunemente adottati sono il sistema **WPA** e il sistema **WPA2** (con AES). Questi due protocolli supportano sia l'autenticazione attraverso una chiave segreta condivisa (***PSK*** = Pre Shared Key) e conosciuta da tutti i client della rete, sia l'autenticazione attraverso un server specifico.

Protocolli per la sicurezza

A grandi linee si può affermare che ai livelli più bassi come il livello 2 collegamento Dati operano protocolli di autenticazione, con il compito di garantire le cosiddette **tre A (AAA, *Autentication, Authorization, Accounting):***

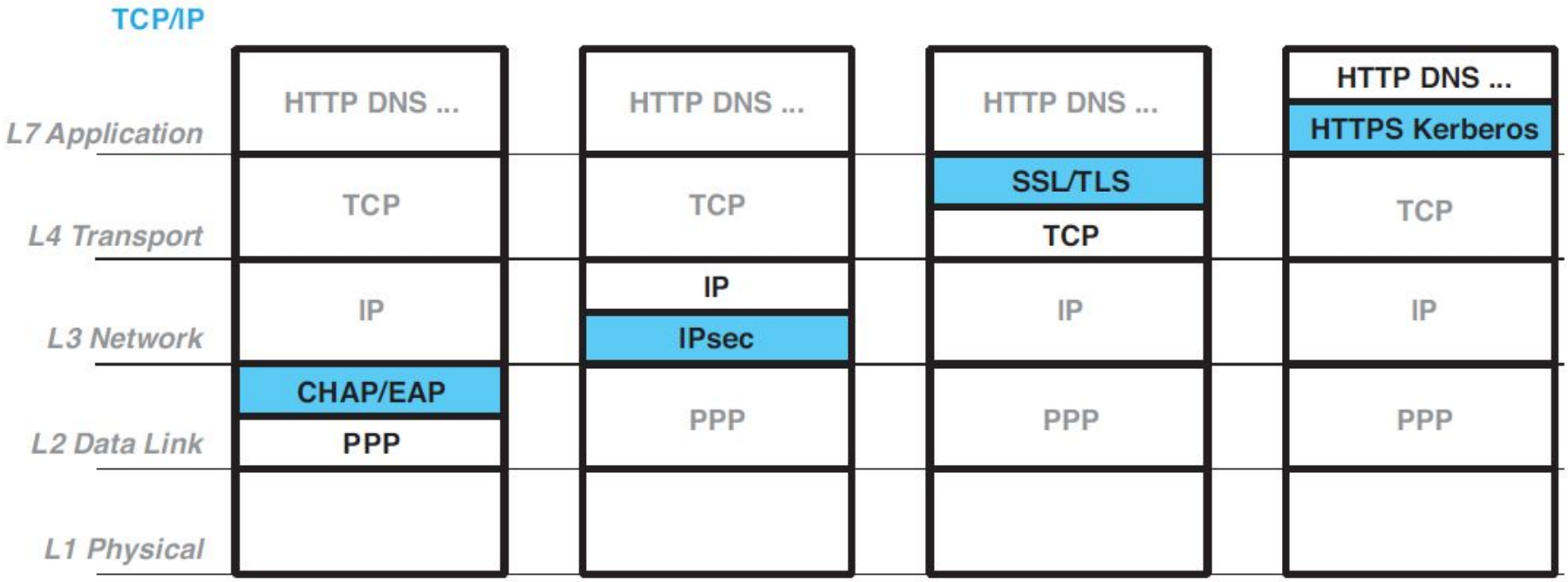
a) ***Autenticazione: garantire la legittimità di un'utenza ed eventualmente la*** sua identità.
b) ***Autorizzazione: concedere all'utente i privilegi di cui gode in base al suo*** profilo.
c) ***Accounting: mantenere traccia delle attività dell'utente.***

Protocolli per la sicurezza

Che le **tre A** vengano verificate sul livello di collegamento Dati è abbastanza ragionevole: in fin dei conti l'accesso a un canale insicuro come una rete avviene quando il protocollo di livello 2 diventa operativo, ovvero quando due host direttamente connessi devono iniziare a comunicare: il momento giusto per autenticarsi è quello.

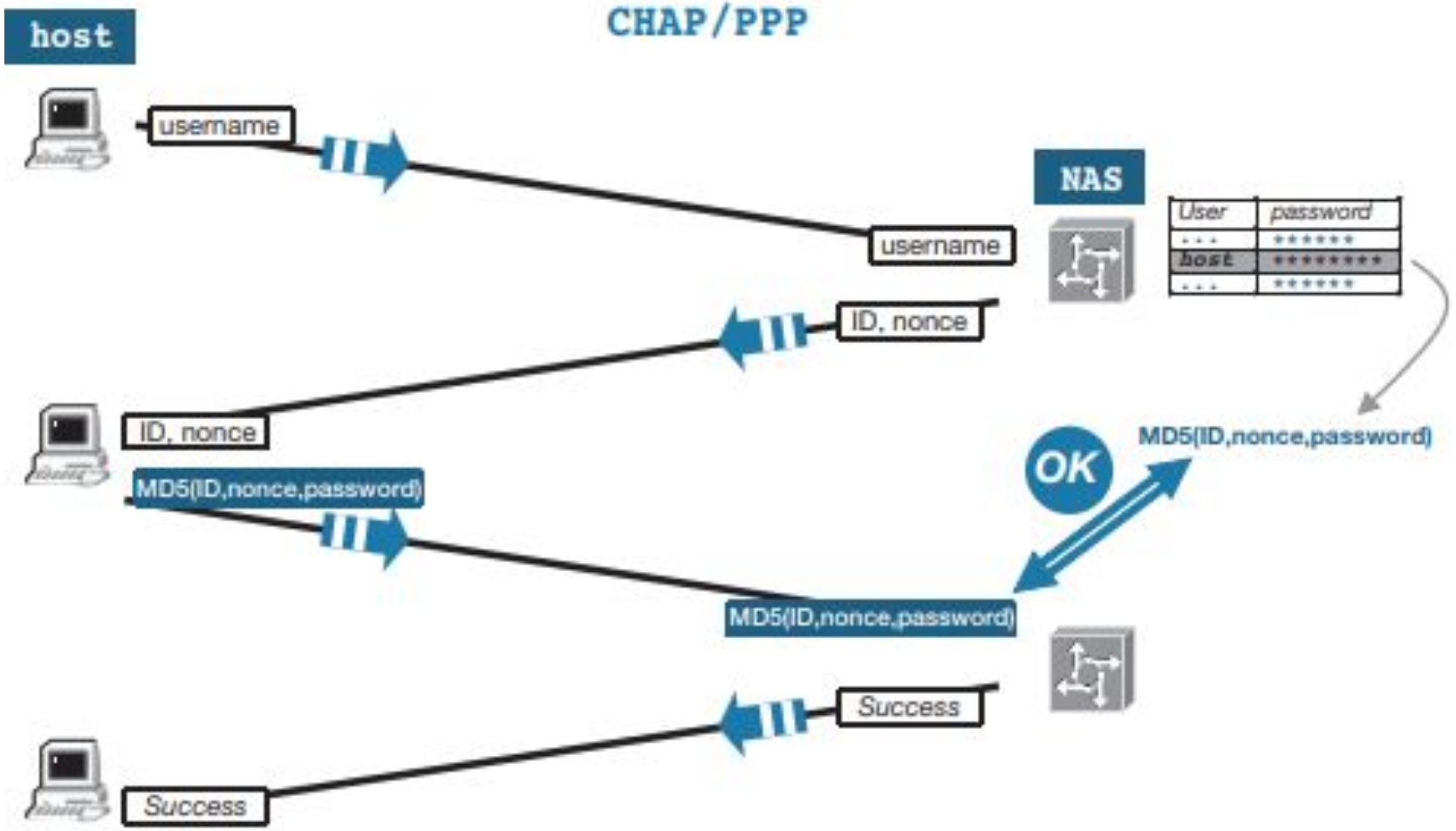
Ai livelli superiori si applicano altri protocolli, ancora di autenticazione quando due applicazioni iniziano a comunicare, ma soprattutto protocolli che devono garantire la segretezza, dato che i contenuti confidenziali che devono essere protetti vengono scambiati a livello 7 Applicazione.

Nello schema vengono messi in risalto i livelli presso i quali operano alcuni dei più diffusi protocolli di sicurezza in una rete.



CHAP/PPP

Challange Handshake Autenticatione Protocoll RFC1994



WPA2

EAP (***Extensible Authentication Protocol, RFC 2284) non è esattamente un*** protocollo ma un framework che può essere usato per implementare protocolli di autenticazione più complessi attuati da appositi SERVER.

L'incapsulamento di EAP per Wi-Fi è interessante e costituisce il modo di autenticazione di una stazione wireless (WT) a un Access Point (AP), autenticazione denominata **WPA2 (*WiFi Protected Access version2)***

WPA *è lo standard precedente****. Lo standard viene ampiamente implementato solo da WPA2***

Sia WPA che WPA2 possono funzionare in due modi: ***enterprise*** *e* ***personal*** *(pensata per applicazioni SOHO).*

WPA2

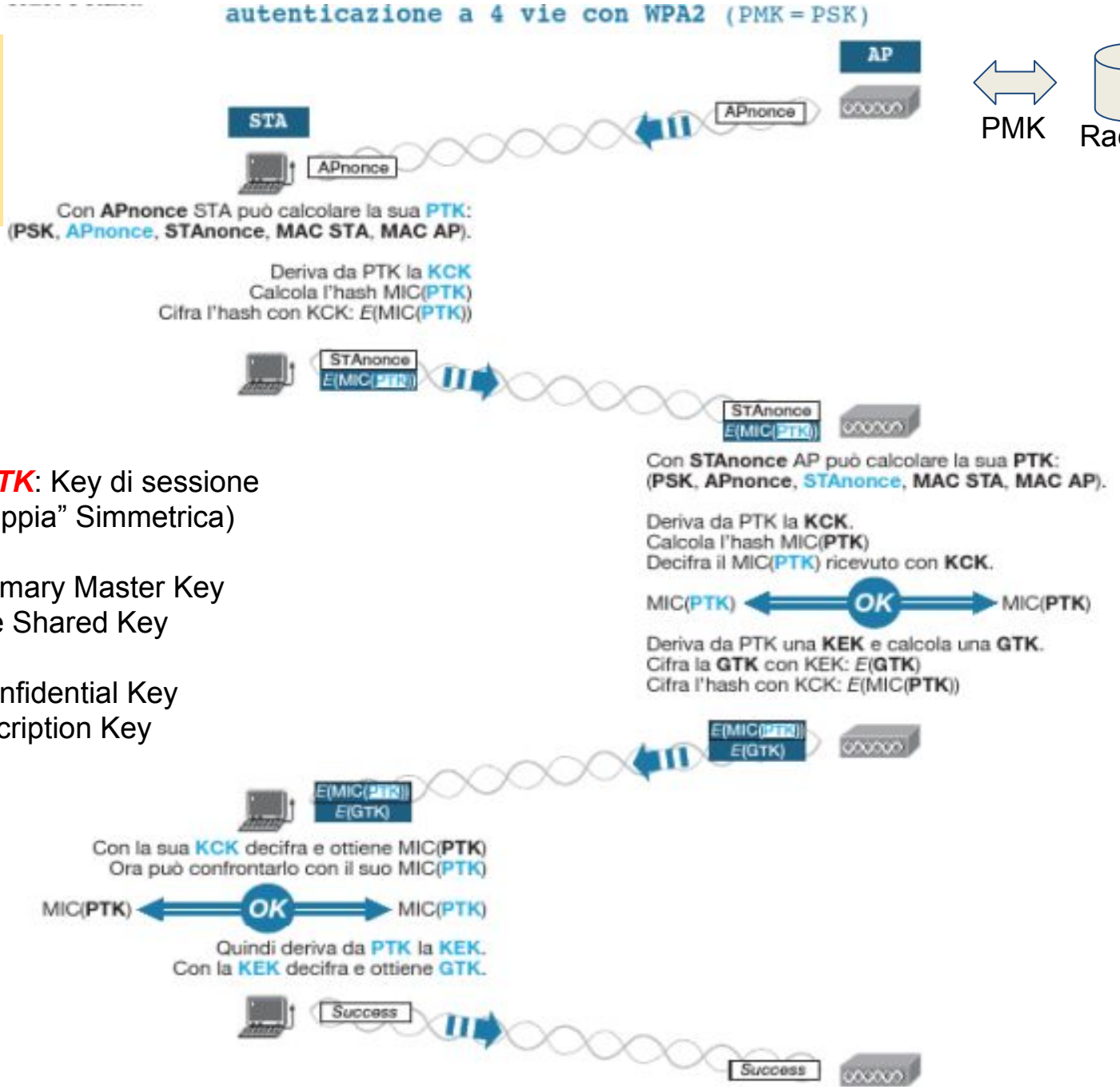
Nel modo **WPA2 *enterprise*** *serve un'altra stazione,* ***il server di autenticazione****,* che contenga le chiavi private segrete degli utenti, dette **PMK (*Primary Master Key). In questo caso ogni utente che si connetterà*** all'AP possiede una chiave Wi-Fi personale. L'AP deve supportare questa funzionalità e deve essere impostato con l'indirizzo IP del PMK(per esempio un server **RADIUS**), nonché con un numero di porta **UDP** e una password d'accesso.

Nel modo ***WPA2 personal*** *invece si usa un segreto condiviso tra stazione* e AP detto **PSK (*Pre-Shared Key), che poi è la password o passprhase Wi-Fi*** preimpostata sull'AP e digitata sulla stazione all'atto della connessione. In questo caso tutti gli host di una rete Wi-Fi condividono la stessa PSK. Nel caso WPA2 *personal, la PMK coincide con la PSK.*

WPA2

Lo scopo è autenticare la stazione WT presso l'access point AP e viceversa, ma anche definire una chiave di sessione per cifrare tutto il flusso delle informazioni sulla connessione wireless che è, per forza di cose, estremamente vulnerabile.

WPA2



PTK **e** ***GTK***: Key di sessione
(***AES*** "doppia" Simmetrica)

PMK: Primary Master Key
PSK: Pre Shared Key

KCK: Confidential Key
KEK: Encription Key

https://www.wired.it/internet/tlc/2017/10/18/come-funziona-attacco-a-wpa2-krack-wifi/

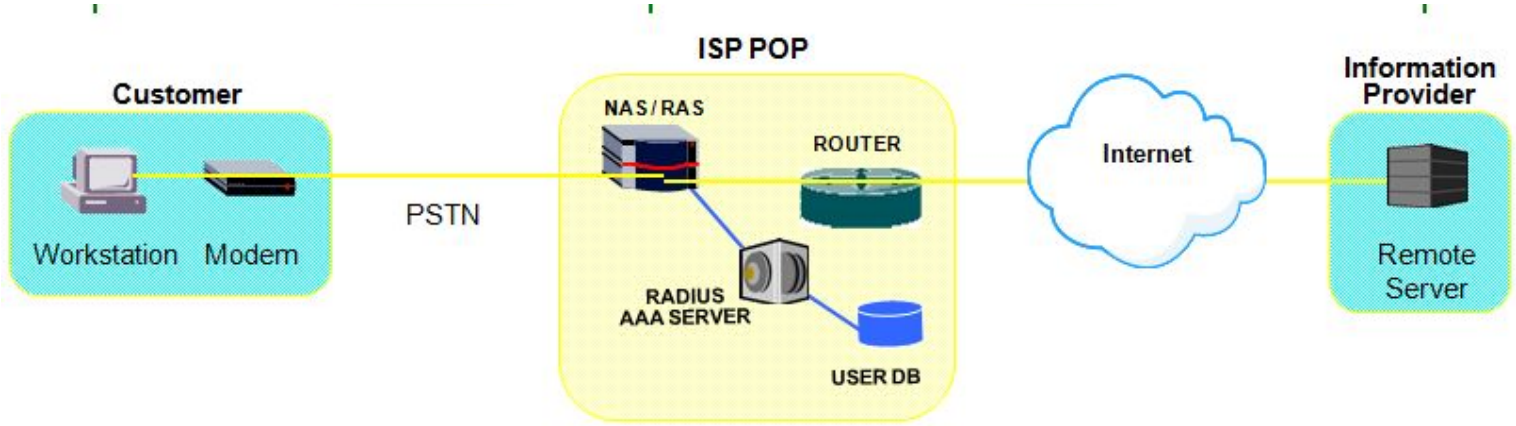
Server Radius

Uno dei modi più comuni per fornire un accesso protetto è l'utilizzo di un server Radius su Debian, per fornire ai protocolli WPA e WPA2 un server di autenticazione in grado di fornire una coppia di credenziali (nome utente / password) diverse per ogni utente della rete wireless.

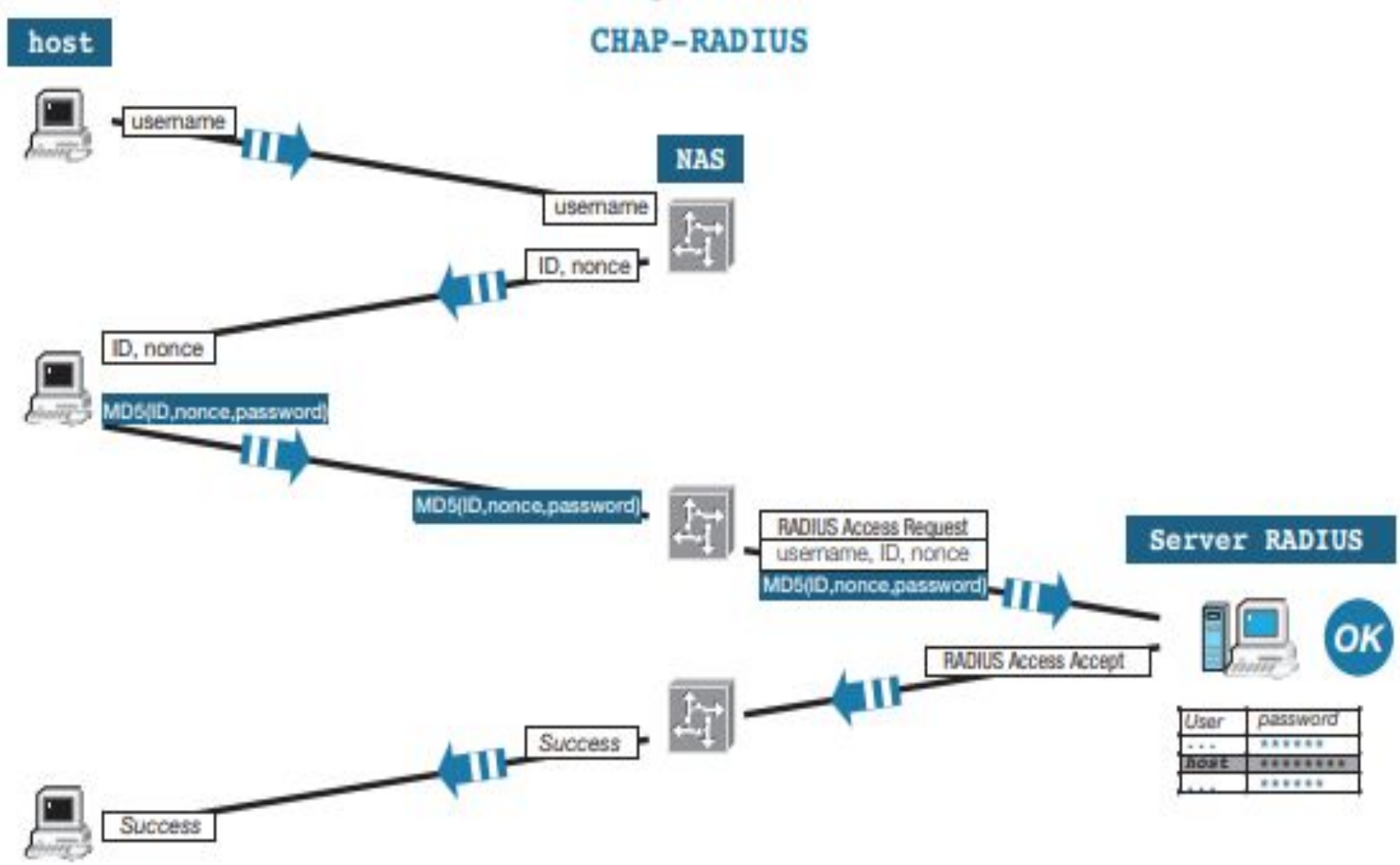
RADIUS è un protocollo client/server di liv.7, trasportato da UDP (porte 1812 e 1823) ma spesso deve agire a liv.2 (PPP/CHAP per ISP o WPA2 per wifi.

Remote Authentication Dial In User Service

Il suo obiettivo è autenticare gli utenti prima di concedere loro l'accesso ad una rete



Server Radius



Authentication

- L'utente o macchina invia una richiesta ad un ***N****etwork* ***A****ccess* ***S****erver* (**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 riguardo all'utente.

Authentication

- 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.
- Il **NAS** riceve la conferma o il rifiuto e lo invia al richiedente

Authentication

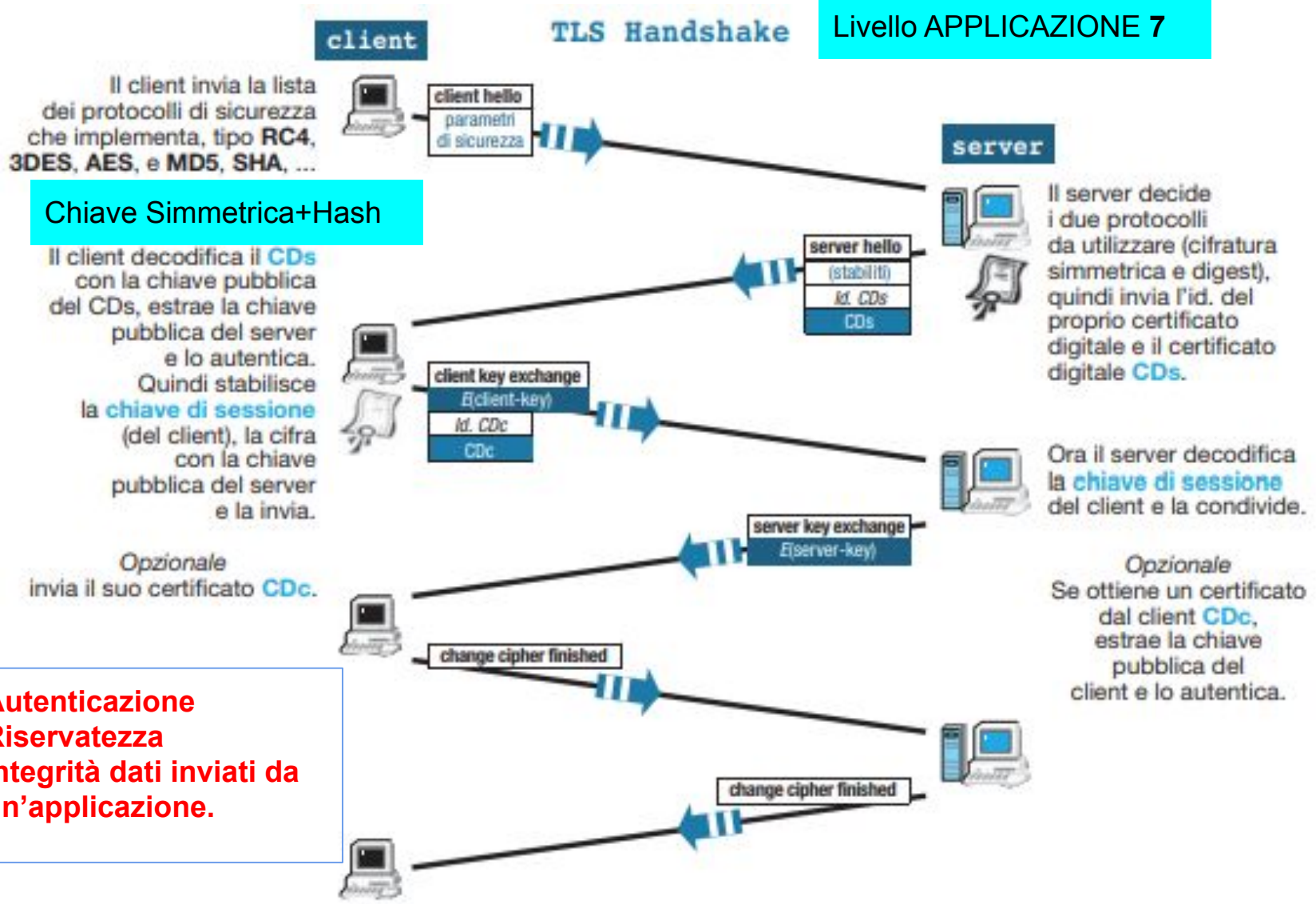
Naturalmente questa è una semplificazione, dal momento che lo scambio di dati deve essere cifrato e i pacchetti che viaggiano hanno una loro struttura definita secondo protocolli specifici. Comunque può essere sufficiente per avere l'idea dell'autenticazione.

Il server Radius serve anche per autorizzare (in base ai ruoli)

SSL/TLS

Transport Layer Security (RFC 5246) / Secure Sockets Layer

Livello APPLICAZIONE **7**

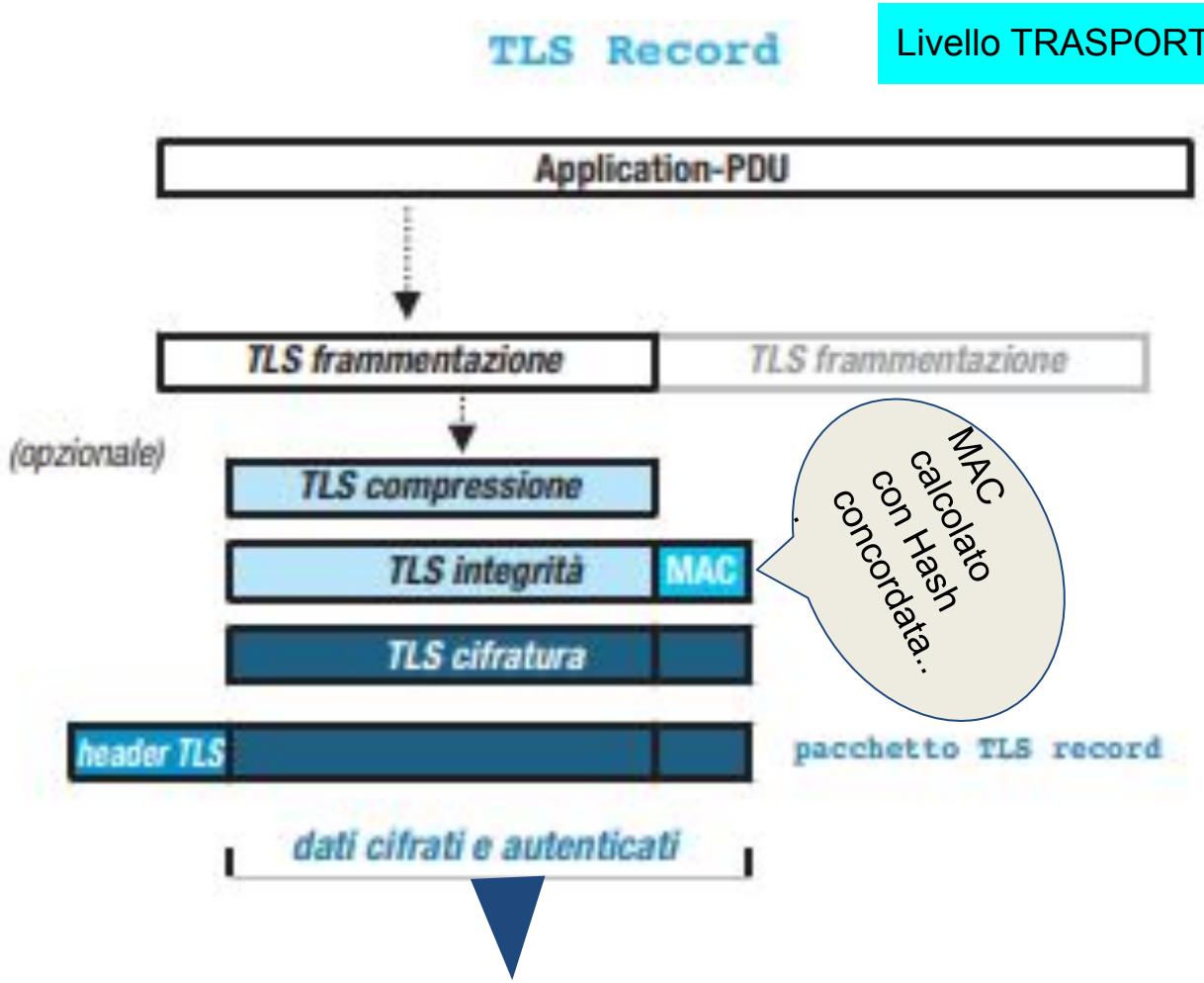


- **Autenticazione**
- **Riservatezza**
- **Integrità dati inviati da un'applicazione.**

SSL/TLS

Transport Layer Security, RFC 5246 / SSL, Secure Sockets Layer

Livello TRASPORTO/SESSIONE**4/5**



Hotspot

Con il termine HotSpot si intende un **punto di accesso ad internet** aperto al pubblico, nel caso degli HotSpot WiFi tale punto di accesso utilizza tecnologie wireless ovvero **senza fili**.

Quando si parla di HotSpot WiFi ci si riferisce ad un'area nella quale è possibile **accedere ad internet**, tale area deve essere creata da **dispositivi programmati appositamente** per offrire un servizio sicuro e controllato. Solitamente gli HotSpot WiFi utilizzano delle antenne per creare delle reti accedibili senza l'ausilio di cablature.

Hotspot wifi: come funzionano

Solitamente gli HotSpot WiFi creano delle **reti aperte** (alle quali chiunque può connettersi senza presentare credenziali) tuttavia una volta all'interno della rete all'utente viene **negato l'accesso ad internet**, egli viene forzato ad una pagina obbligata. L'HotSpot WiFi gli negherà qualunque comunicazione esterna fintanto che l'utente in questione non si sarà **autenticato**. In questo modo sarà possibile deresponsabilizzare il proprietario della rete dalle azioni dei suoi clienti.

Hotspot wifi: a cosa servono

Gli HotSpot WiFi sono stati progettati per diversi utilizzi:

Utilità: In un mondo in continua evoluzione, dove la possibilità di avere dispositivi in grado di navigare in rete è ormai una comune realtà quotidiana l'**esigenza** di disporre di un punto d'**accesso ad Internet** a banda larga gratuito, facile e sicuro sembra essere un **requisito indispensabile**. Gli HotSpot WiFi sono progettati proprio per far fronte a questa esigenza e risolvere tutte le problematiche tecniche e legali legate a questo tipo di servizio.

Hotspot wifi: a cosa servono

Gli HotSpot WiFi sono stati progettati per diversi utilizzi:

Sicurezza: Permettere a clienti e turisti di navigare gratuitamente è sicuramente una grande **spinta** per ogni attività, ma quali sono i **rischi**? Oggi giorno sappiamo benissimo come attraverso internet vengano veicolate **truffe telematiche**, **violazioni di copyright** o **condivisioni di materiali illeciti**: e se qualcuno utilizzasse la nostra connessione per farlo? Se qualcuno connesso alla nostra rete riuscisse ad intercettare delle nostre **informazioni private**?
Gli HotSpot WiFi nascono proprio per **isolare** la rete del gestore da quella dell'utente e per tener traccia delle identità di coloro che navigano.