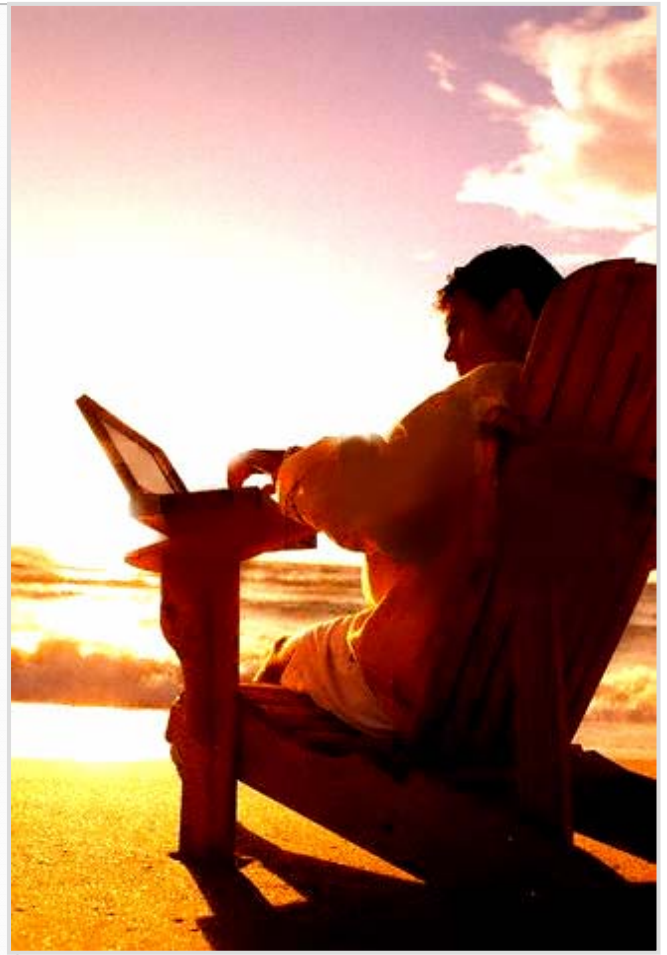
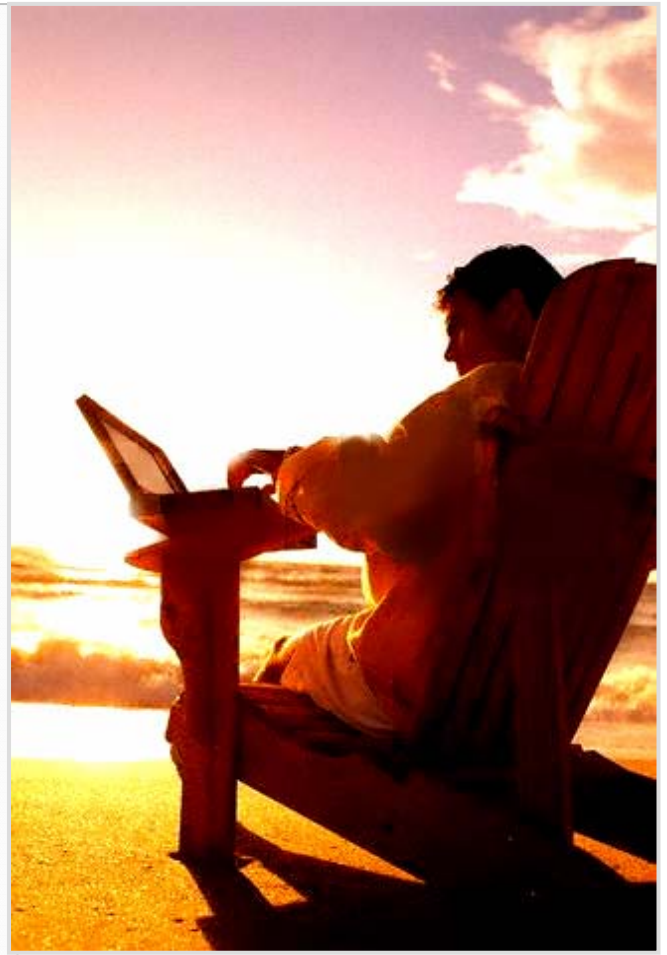
linkem
keep in touch

UNIROMA3 – Architettura di rete di un WISP

Ing. Maurizio Martinoli





keep in touch

2001

Nasce Megabeam Italia S.p.A, primo Wireless Internet Provider nello scenario TLC italiano. La sua missione è quella di "offrire servizi di connessione per la trasmissione di dati e voce tramite tecnologia wireless, raggiungendo luoghi nei quali non è disponibile la banda larga o nei quali è possibile promuoverne un uso più efficiente".

2003

Inizia la commercializzazione del servizio Wi-Fi Megabeam nelle location più prestigiose (aeroporti, hotel, centri congresso).

2004

Megabeam Italia S.p.A, raggiunge il break-even, risultato consolidato da un aumento di capitale sociale. Nasce la divisione Hot Zone: l'obiettivo della business divisione è portare la banda larga nelle aree geografiche affette dal ***digital divide***.

2005

Megabeam lancia il nuovo brand aziendale **LINKEM**

Attualmente LINKEM è leader nazionale
nella realizzazione di reti per la connessione a banda larga
in modalita' wireless (senza fili) su protocolli innovativi (Wi-Fi e Hiperlan)

linkem

linkem
keep in touch

Attualmente LINKEM fornisce i suoi servizi in due macro aree di business per cui sono state approntate due business unit dedicate

- **HOTSPOT:** all'interno di aeroporti, catene alberghiere e centri congressi, dando a chi viaggia la possibilità di connettersi ad alta velocità, attraverso il proprio portatile, non solo ad Internet ma anche alla propria Lan aziendale (Wi-Fi)

- **HOTZONE:** all'interno di aree comunali, distretti industriali, Comunità Montane, Province, portando la banda larga ed i suoi applicativi dove non arriva, in modo efficace ed efficiente.

IL NETWORK DI HOTSPOT

keep in touch

SALE VIP AEROPORTUALI

Alitalia

AEROPORTI

AEROPORTI DI MILANO
LINATE E MALPENSA

Aeroporti di Roma

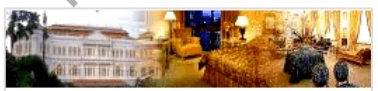
AEROPORTO FRIULI-VENEZIA GIULIA

SAVE

AEROPORTO DI GENOVA

AEROPORTI SISTEMA DEL GARDA
Verona Brescia

HOTEL



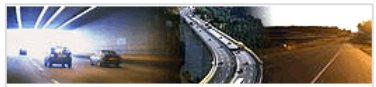
Best Western

PREGIO hotels

HOTEL INDIPENDENTI

LINKEM
vanta un network di Hotspot strategici
e coerenti con le esigenze del target client,
che rappresentano un valore per i propri partner
e per l'effettivo utilizzo del servizio
da parte dell'end user

AREE DI SERVIZIO AUTOSTRADALI



autostrade per l'italia

A1 - A4

PORTI TURISTICI

Viareggio

Tropea

San Rocco

Punta Ala

Santa Mara di Leuca

SALE CONGRESSO

Musica per Roma

AUDITORIUM PARCO DELLA MUSICA

C.E.T. Centro Europeo di Toscanini

linkem
keep in touch

keep in touch

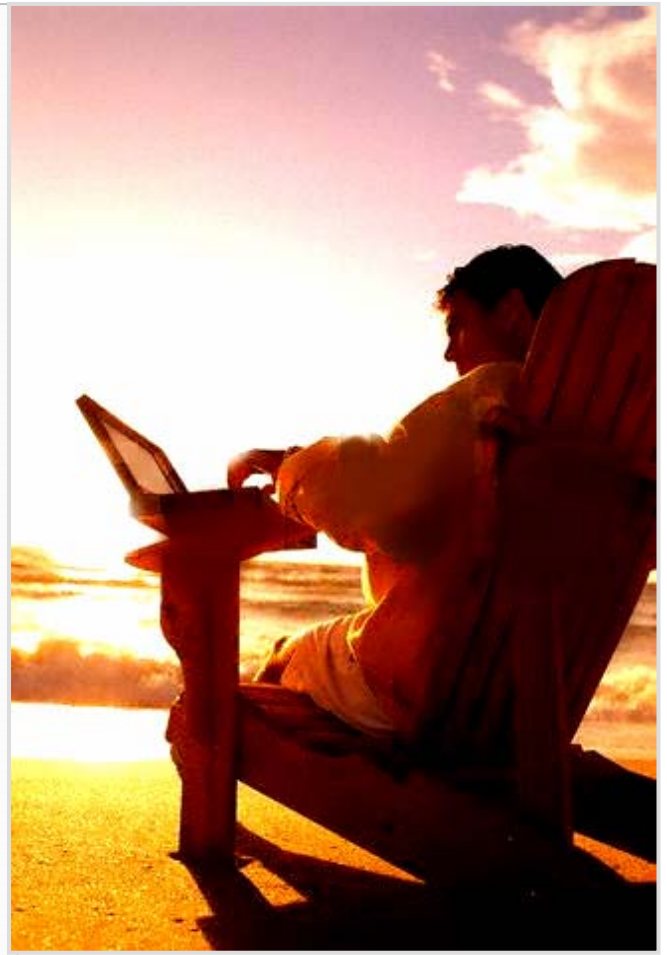
linkem HOTZONE

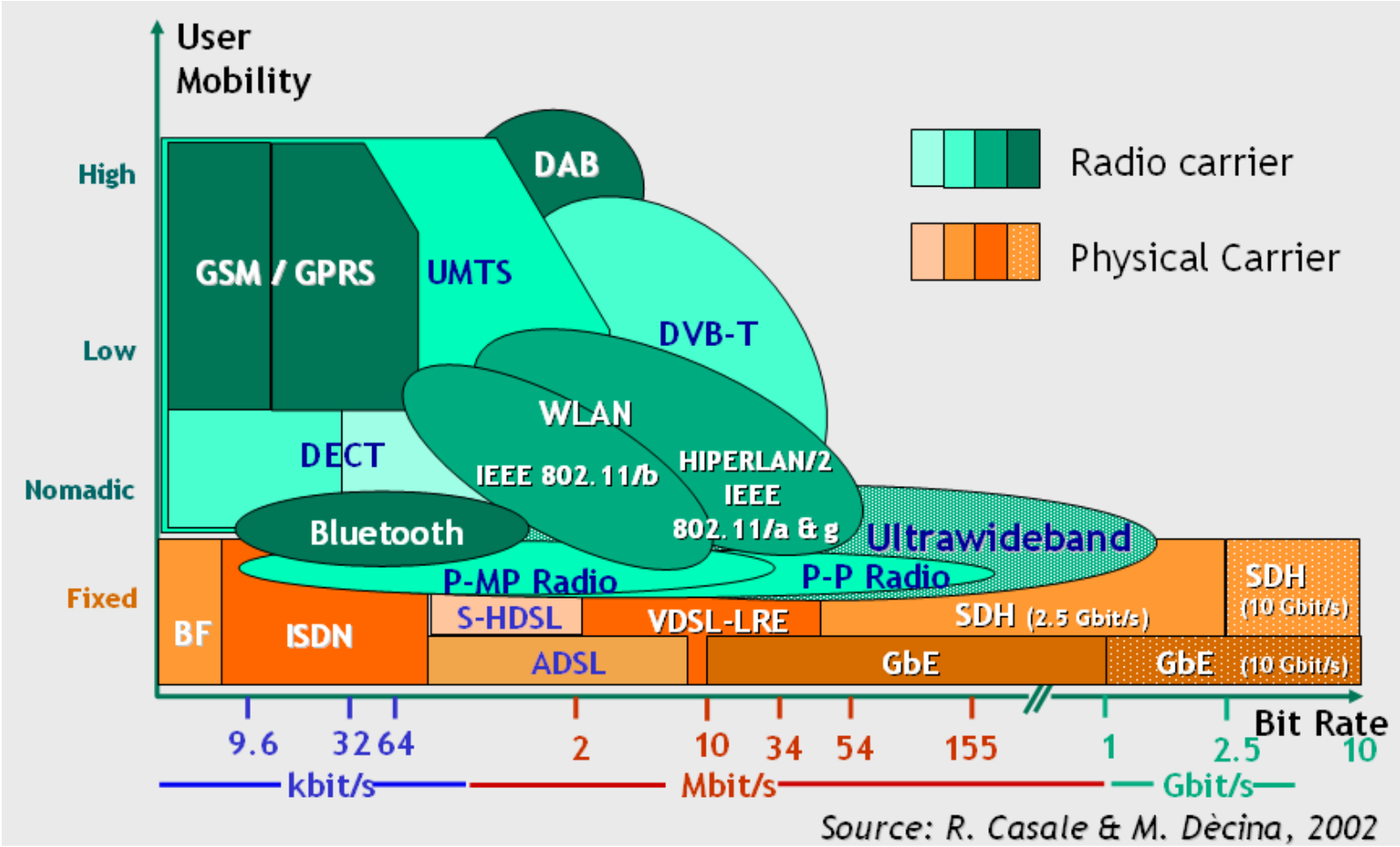
Business Proposition

Portare la Banda Larga in modalità Wireless dove ancora non arriva
(Piccoli Comuni, Comunita' Montane, Distretti Industriali in aree disagiate, Province)

Aprire la banda larga (già presente) a più utenti tramite soluzioni Wireless:
(Comuni, Distretti Industriali)

Creare connessioni "Intranet" fra diversi edifici
(di uno stesso Comune e/o Comuni limitrofi)





CSMA/CA – *Carrier Sense Multiple Access con Collision Avoidance*
Già ben noto in protocolli commercializzati da decine di anni, come l'802.3 (ethernet)

In un ambiente wireless non è possibile assumere che una stazione sia in grado di sentire l'attività di tutte le altre.
Se una stazione che vuole trasmettere rileva la non occupazione del mezzo, non necessariamente significa che il mezzo sia libero attorno all'area di ricezione.

Collision avoidance + positive aknowledgment

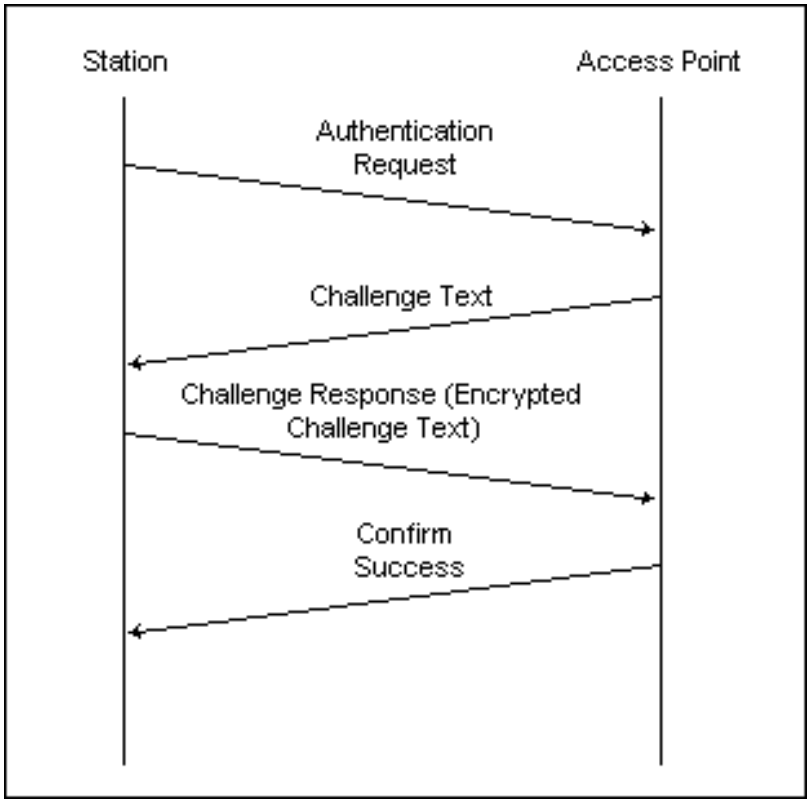
802.3
La stazione testa il mezzo trasmissivo. Se occupato non trasmette.
Se libero per un tempo detto DIFS (Distributed Inter Frame Space) allora la stazione comincia la trasmissione.
La stazione ricevente controlla il CRC del pacchetto ricevuto e invia un pacchetto di acknowledgement (ACK).
Se non riceve un ACK la stazione ritrasmette fino ad un massimo numero di ritrasmissioni (definite dallo standard)

Virtual carrier sense

La stazione che vuole trasmettere invia un pacchetto RTS (Ready To Send).
La stazione di destinazione invia un pacchetto CTS (Clear To Send) se il mezzo è libero.

Tutte le stazioni ricevendo sia un RTS che un CTS, impostano l'indicatore *Virtual Carrier Sense* (chiamato *NAV* che sta per *Network Allocation Vecto*r), per un certo tempo ed utilizzano questa informazione, insieme con il Phisycal Carrier Sense, al momento in cui vanno a effettuare la rilevazione di occupazione del mezzo.

Questo meccanismo riduce la probabilità di collisione su un'area di ricezione, che è nascosta all'interno dell'intervallo di tempo necessario alla trasmissione dell'RTS.
La stazione riceve il CTS e definisce il mezzo come occupato fino alla fine della trasmissione.



L'access point invia un testo di sfida (challenge text) al client che dovrà decrittarlo con la giusta chiave e rispedirlo all'access point. La chiave è contenuta in un attributo MIB di sola scrittura attraverso un MAC management path (dentro il MAC).

802.11b
2.4 GHz (ISM). Velocità fino a 11mbps.
Il suo successo è dovuto alla standardizzazione voluta dal WECA.

802.11a
5 GHz. Velocità fino a 54 mbps.
L'802.11a non è compatibile con l'802.11b ma possono essere create delle soluzioni di bridging tra i due protocolli.

802.11g
2.4 GHz (ISM). Velocità fino a 54 mbps.
L'802.11g è compatibile con l'802.11b e offre una maggiore velocità di accesso.

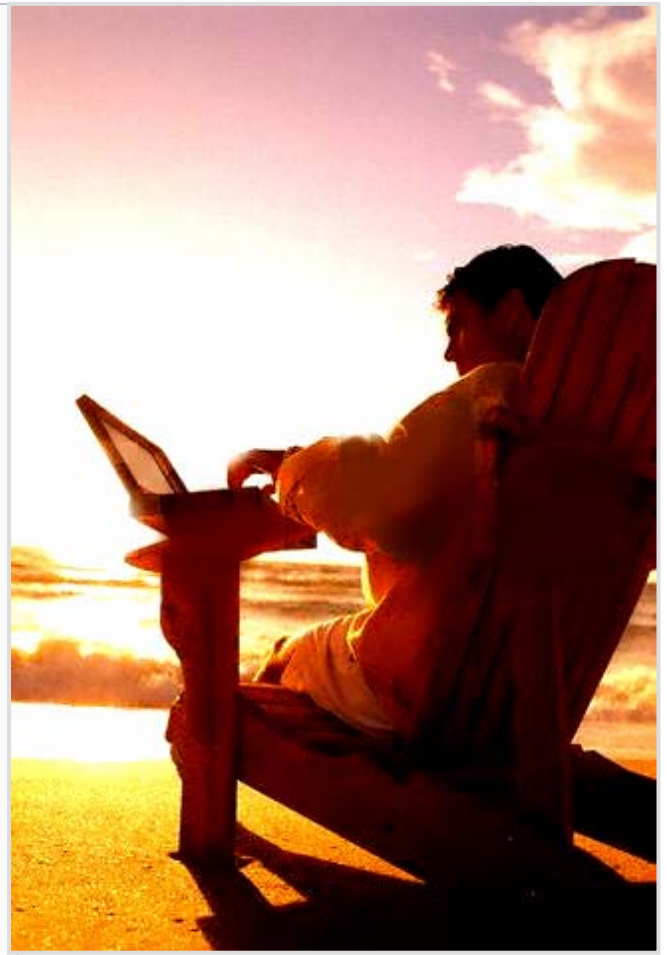
802.11e
Introduce miglioramenti a livello di QoS per applicazioni realtime.

802.11h

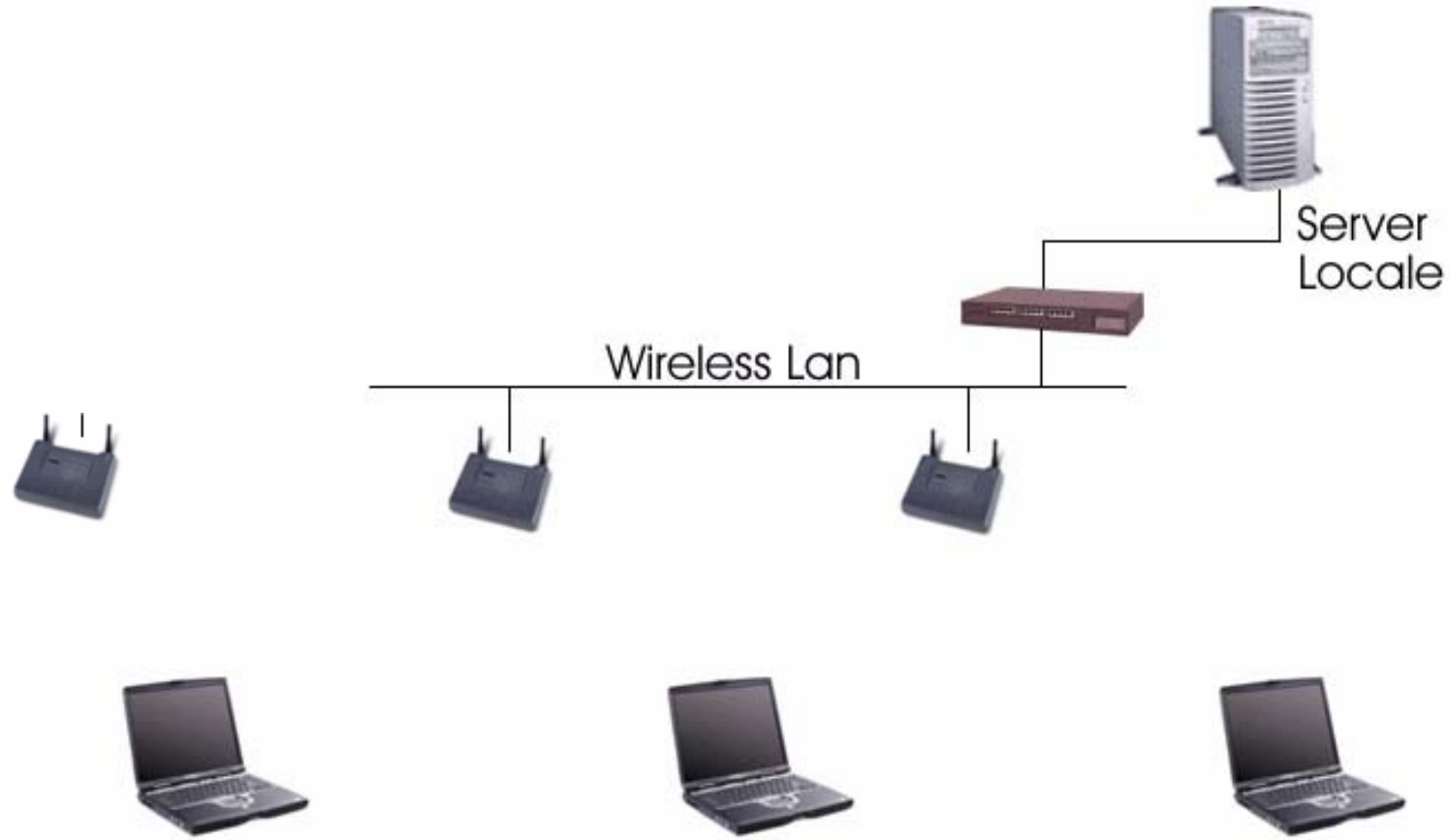
Prevede miglioramenti sull'esistente 802.11a, ovvero la coesistenza con altri servizi che lavorano a 5Ghz come l'HyperLAN2.
Importante nella comunità europea che sta spingendo molto la promozione dello standard dell'HyperLAN2 per le WLAN.

802.11i

Gestisce miglioramenti relativi alla sicurezza.
Lo scopo principale dell'802.11i è quello di rimpiazzare il WEP con un nuovo standard chiamato Temporal Key Integrity Protocol (TKIP).



ARCHITETTURA LOCALE

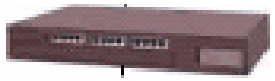


ARCHITETTURA LOCALE - COMPONENTI

Server locale (NAS)
- DHCP
- Web server
- DNS
- RADIUS client
- Routing

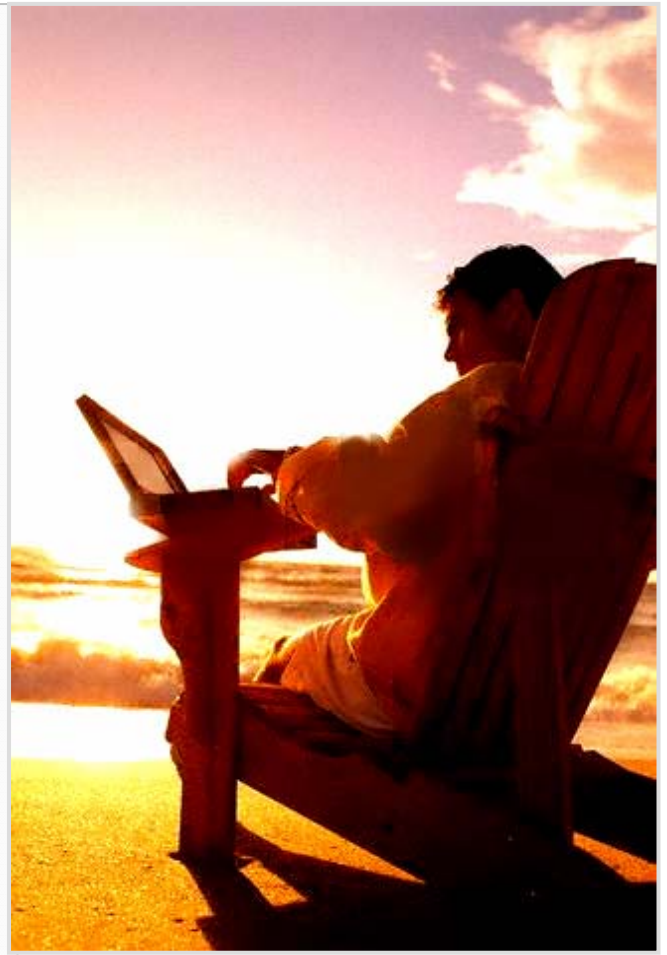
(CLI over Linux)

Access Point
- WiFi Compliant
- Livello 2
- 802.11 b/g (a)
- 802.1x



Switch
- Smart switch
- Livello 2
- VLAN capable

Client
- WiFi capable
- Internet browser capable
- OS indipendent



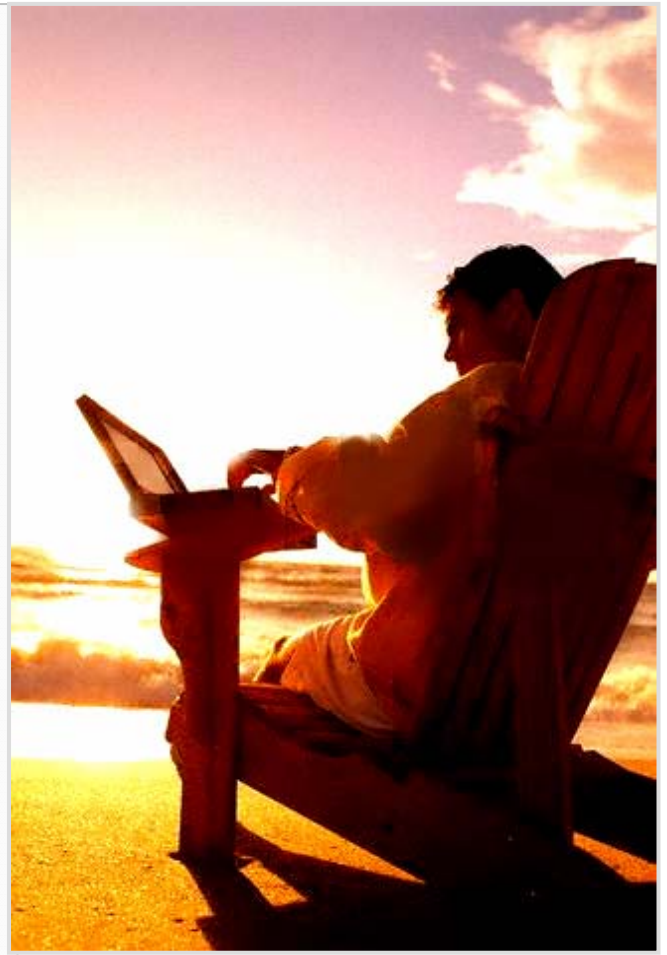
DHCP - *Dynamic Host Configuration Protocol*
Il protocollo usato per assegnare gli indirizzi IP ai calcolatori di una rete

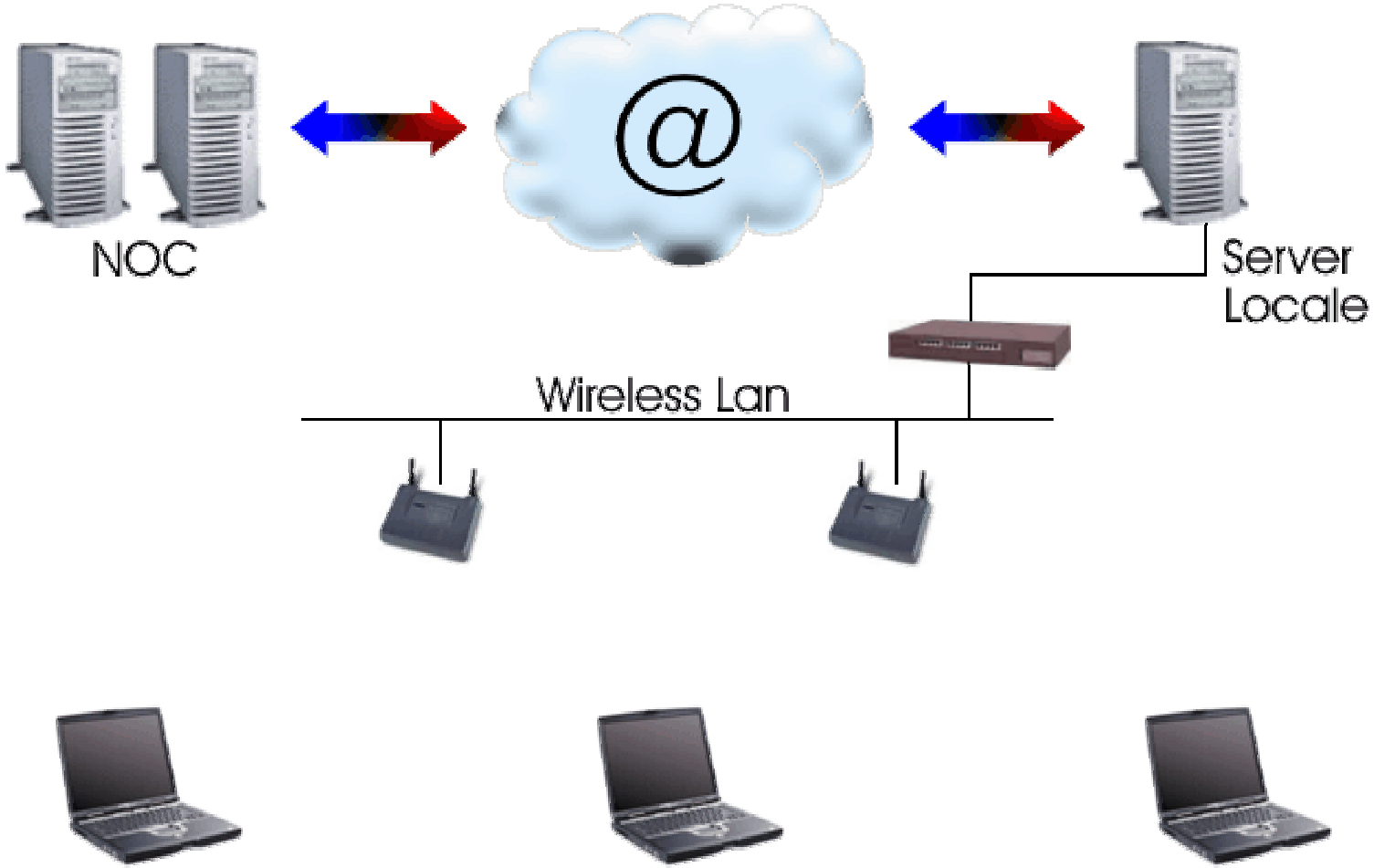
DNS – *Domain Name Service*
Il DNS è un servizio di directory, utilizzato per la risoluzione di nomi di Host in indirizzi IP

Smart Switch
- supporto di più istanze del protocollo Spanning Tree
- supporto di LAN virtuali (VLANs) secondo lo standard 802.1Q
- mirroring delle porte
- supporto della QoS (Quality of Service)

WiFi – *Wireless Fidelity*
Nome commerciale delle reti locali senza fili (WLAN) basate sulle specifiche IEEE 802.11 (a/b/g)

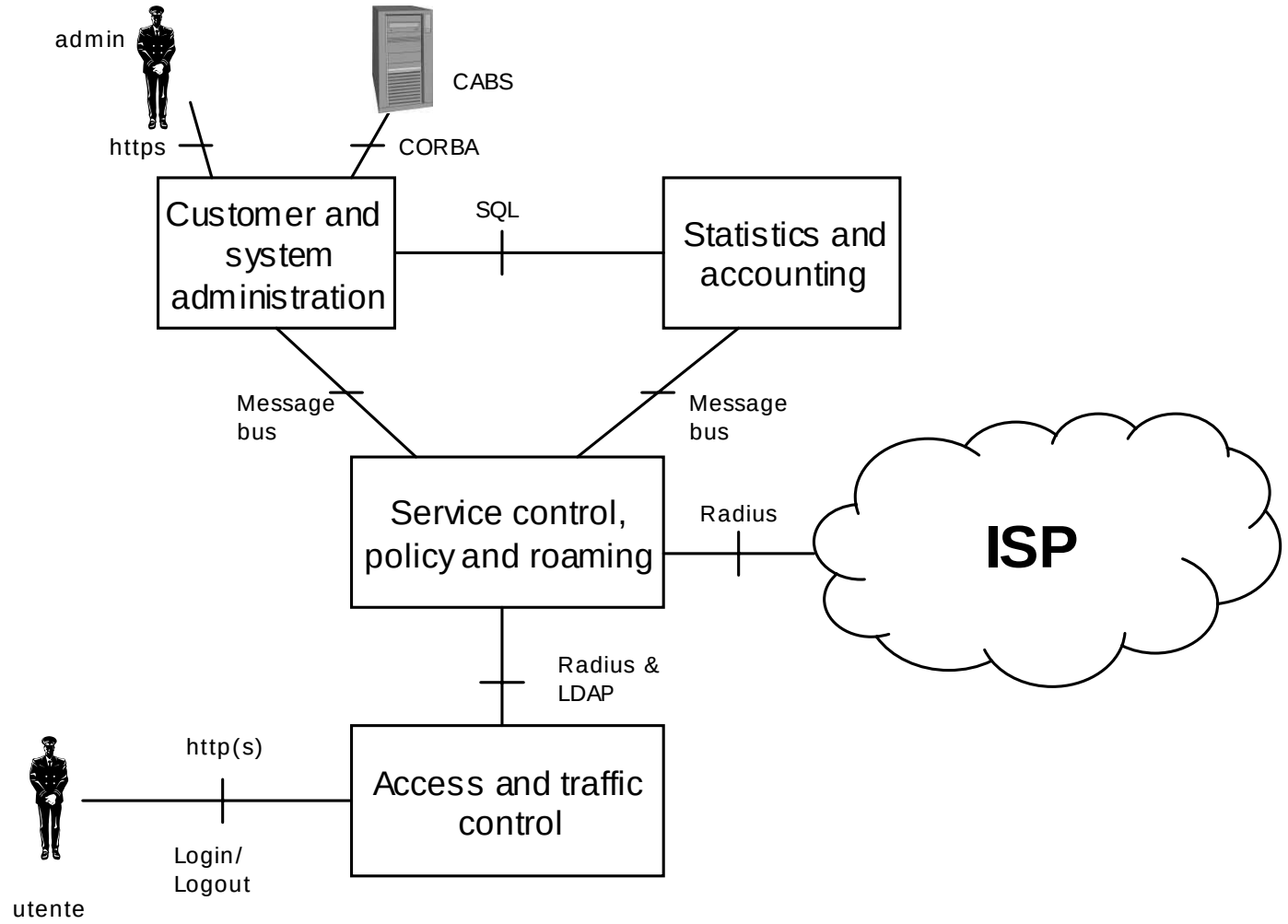
Access point:
- Capacità massima 16 SSID
- Supporto VLAN (Ingress & Egress)
- Supporto del Quality of Service (o QoS) diverso per ogni SSID
- Configurazione della sicurezza (802.1x,WEP,WPA,MAC) diversa per ogni SSID
- Selezione dei canali manuale e automatica
- Selezione della potenza radio manuale e automatica
- Supporto VLAN (diverso per ogni SSID e per ogni utente)
- Configurazione via Web sicuro (SSL), via SNMP e tramite CLI
- WDS (multipoint wireless bridging)
- Rilevamento dei dispositivi non autorizzati (Rogue AP)

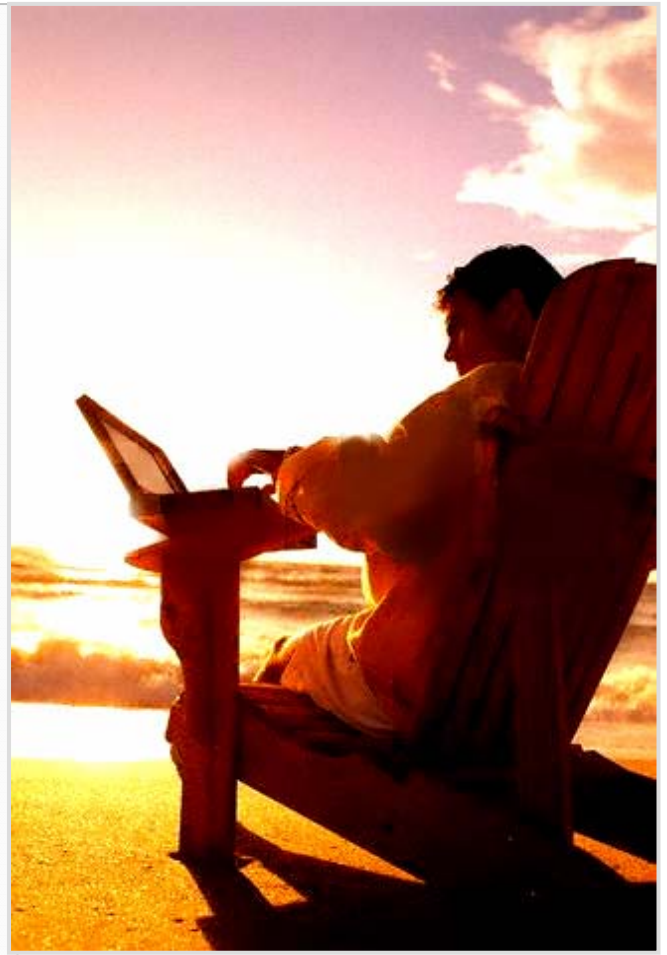




NOC: *Network Operation Center*

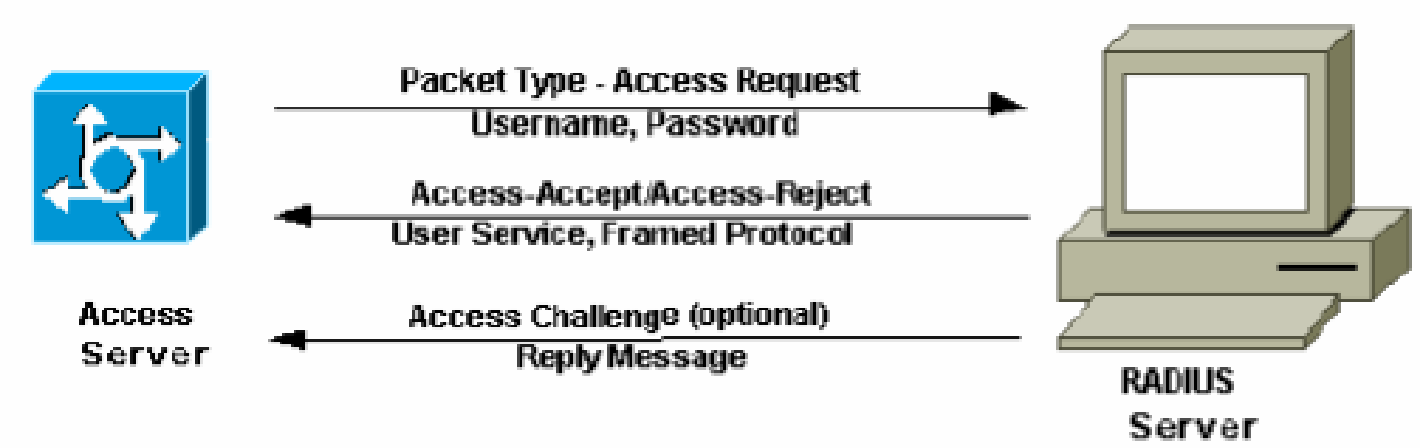
- 2 server RADIUS che lavorano in ridondanza (CLI over Linux)
- 1 server RADIUS dedicato al roaming (CLI over Linux)
- 1 server per l'accounting (BSD)
- 1 server per l'authorization (BSD)
- 1 server per l'interfaccia GUI (Linux RedHat, Tomcat, JSP)





RADIUS - Remote Access Dial In User Service (RFC 2138)

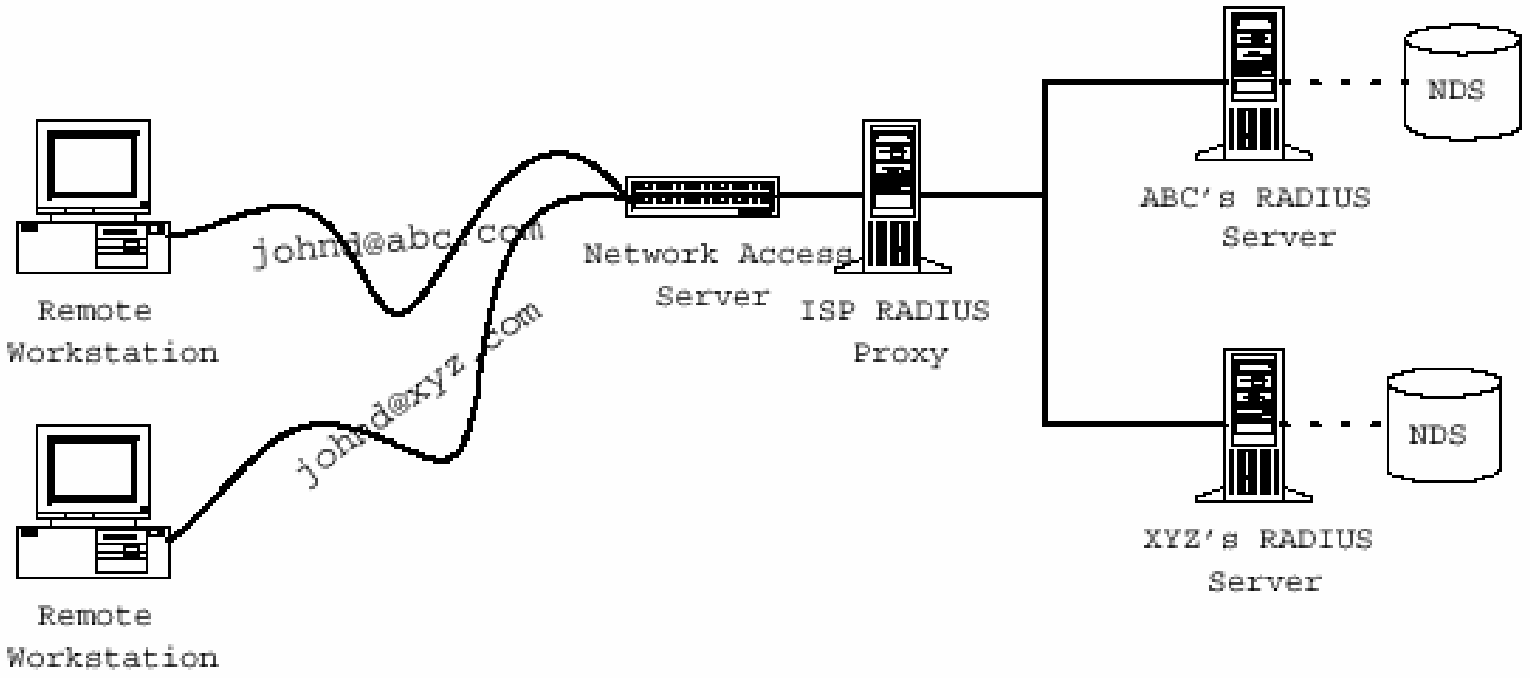
Metodo di autenticazione per utenti che necessitano di accesso alla rete da una location remota.



-L’utente inizializza l’autenticazione PPP verso il NAS (1)
- Il NAS richiede lo username e la password (se PAP) oppure il challenge (se CHAP) (2)
- L’utente risponde (3)
- Il client RADIUS invia username e la password crittografata al server RADIUS (4)
- Il server RADIUS risponde con Accept, Reject o Challenge (5)
- Il client RADIUS si comporta in base alle informazioni presenti all’interno dei messaggi Accept o Reject

Il pacchetto Access-Request contiene lo username e la password crittografata, l’indirizzo IP del NAS e la porta

ARCHITETTURA WAN – RADIUS PROXY



SICUREZZA

- Password dell'utente crittografata mediante l'algoritmo MD5
- Comunicazioni tra i vari RADIUS cifrati mediante uno "shared secret" che viene impostato manualmente sui dispositivi (non viaggia mai sulla rete)

- IPSEC: per cifrare tutte le comunicazione tra più server RADIUS; è possibile gestirlo tramite router o tramite demone appositamente installato sul server.

Standard di livello 3 per ottenere connessioni sicure *portal-to-portal* basate su IP (RFC 2401-2412)

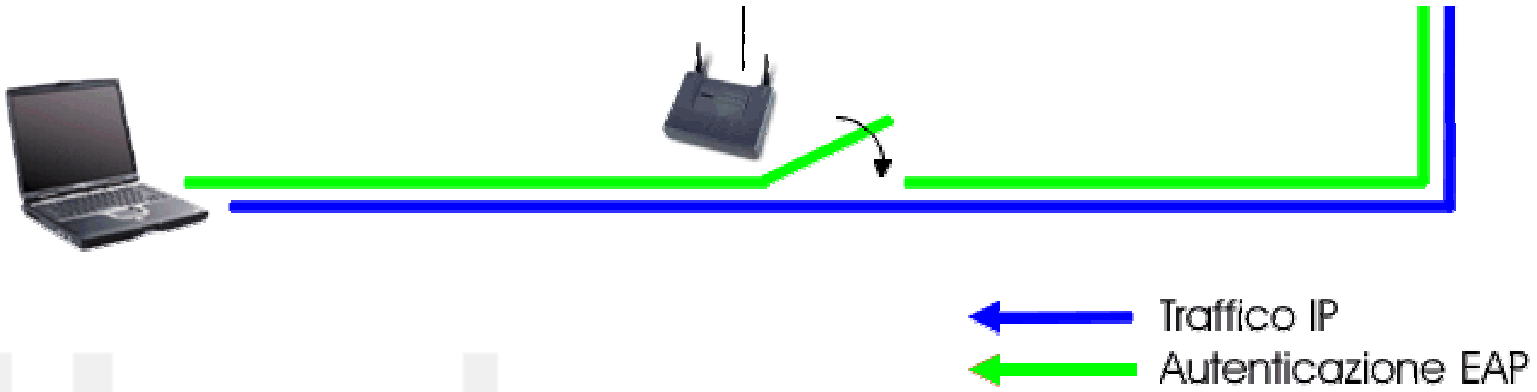
IPsec è una collezione di protocolli formata da:
-Protocolli che forniscono la cifratura del flusso di dati
AH: garantisce l'autenticazione e l'integrità del messaggio ma non offre la confidenzialità
ESP: fornisce autenticazione, confidenzialità e controllo di integrità del messaggio

-Protocolli che implementano lo *scambio delle chiavi* per realizzare il flusso crittografato
IKE: Internet key exchange, èun protocollo di livello applicazione e utilizza il protocollo UDP come protocollo di trasporto

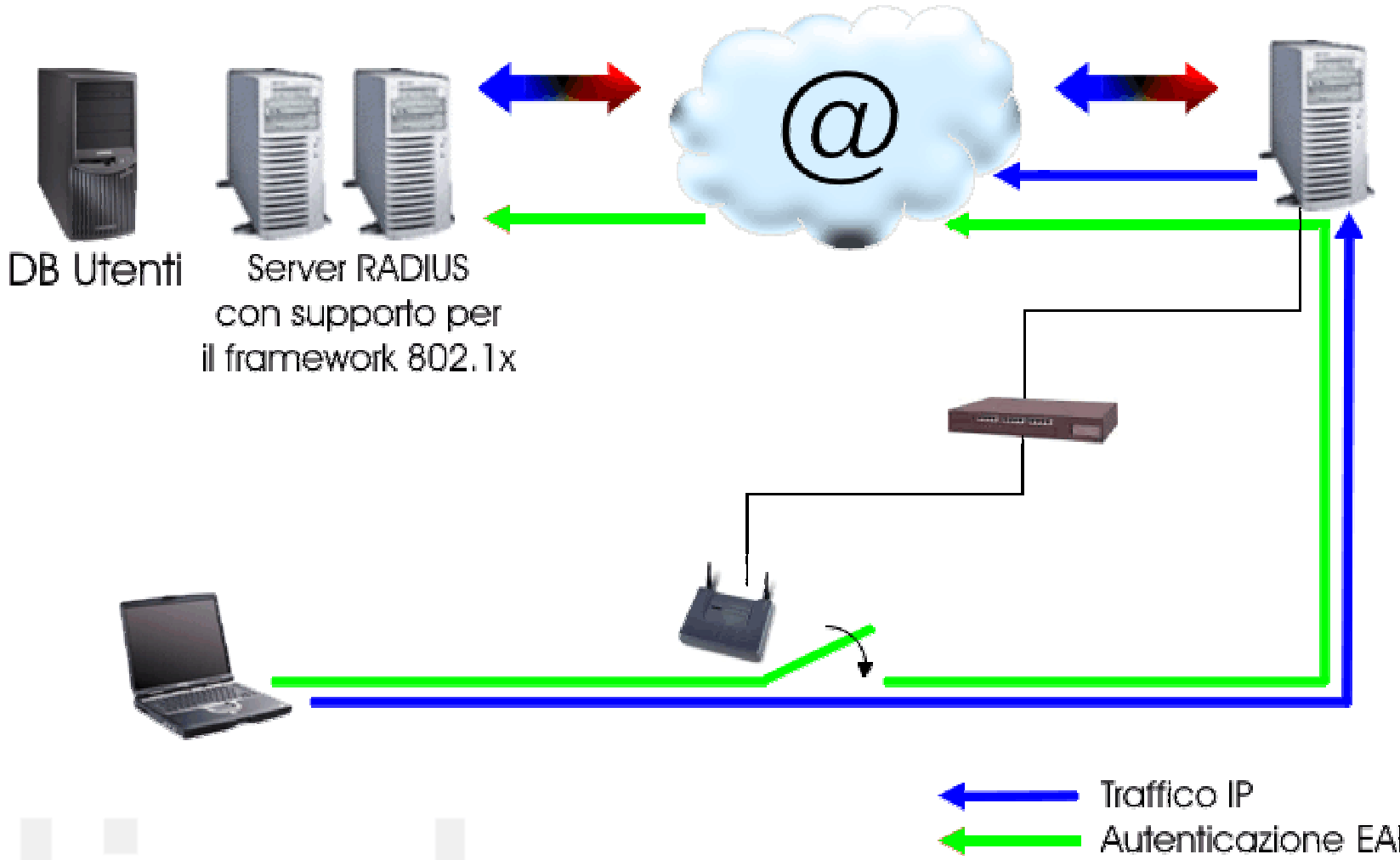
Tunnel mode: tutto il pacchetto è incapsulato in un nuovo pacchetto
Transport mode: solo il payload del pacchetto

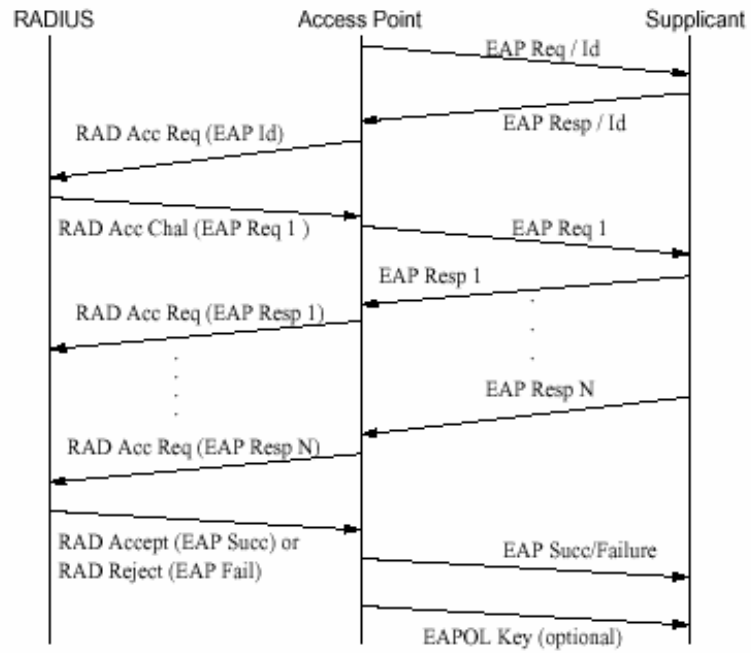
802.1x – *EAP* *(Extensible Authentication Protocol)*

EAP/MD5*: analogo al metodo CHAP, utilizzo di un algoritmo di tipo hash combinato ad uno shared secret*
EAP/TLS*: utilizzo di certificati su lato client e server*
EAP/TTLS*: creazione di un tunnel di cifratura tra client e server*
PEAP*: simile al TTLS, solo supporto di metodi EAP*
LEAP*: protocollo proprietario della Cisco utilizzabile solo con dispositivi Cisco*
EAP/SIM*: utilizzo della SIM card per il controllo di accesso*



Metodo EAP	Chiavi dinamiche	Mutua autenticazione	Username Password	Metodi di attacco	Commenti
EAP-MD5	No	No	Sì	- Attacchi da dizionario - Man in the middle - Furto della sessione	- Facile da implementare - Supportato su molti server - Non sicuro - Richiede db
EAP-TLS	Sì	Sì	No	- Livello di sicurezza elevato	- Richiede certificati su client - Oneroso
EAP-TTLS	Sì	Sì	No	- Livello di sicurezza elevato	- Creazione di un tunnel SSL - Supporto di altri metodi come il PAP e CHAP - L'identità dell'utente è protetta
PEAP	Sì	Sì	No	- Livello di sicurezza elevato	- Simile al TTLS - Creazione di un tunnel SSL - Non supporta PAP e CHAP
LEAP	Sì	Sì	Sì	- Attacchi da dizionario	- Soluzione proprietaria - L'AP deve supportare LEAP

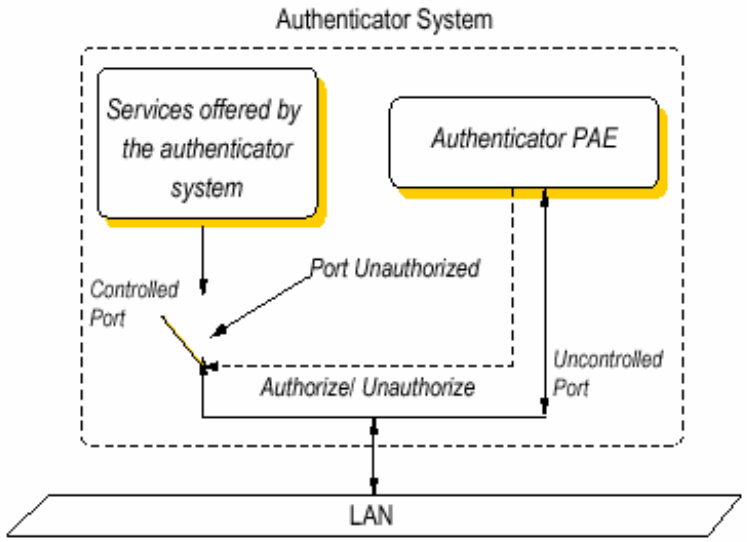




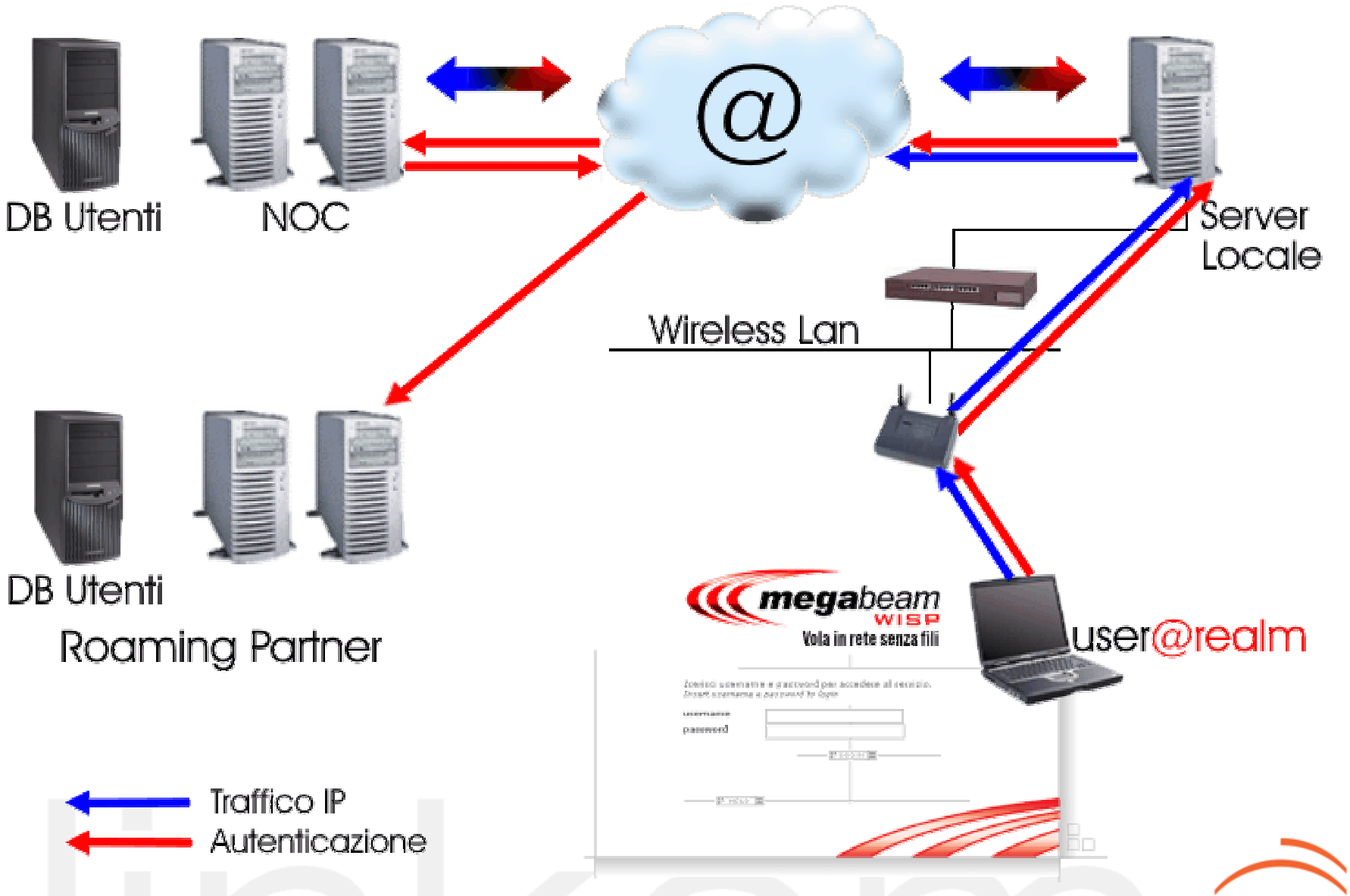
Opera a livello di rete piuttosto che a livello data-link.

Il messaggio EAP Request contenente un challenge text viene inviato al supplicant che deve rispondere utilizzando l'EAP Response.

Protocollo estensibile.



Il sistema autenticatore ha due porte di accesso alla rete: l'*Uncontrolled port* e la *Controlled port*. La porta Uncontrolled filtra tutto il traffico di rete e concede l'accesso solo ai pacchetti EAP.

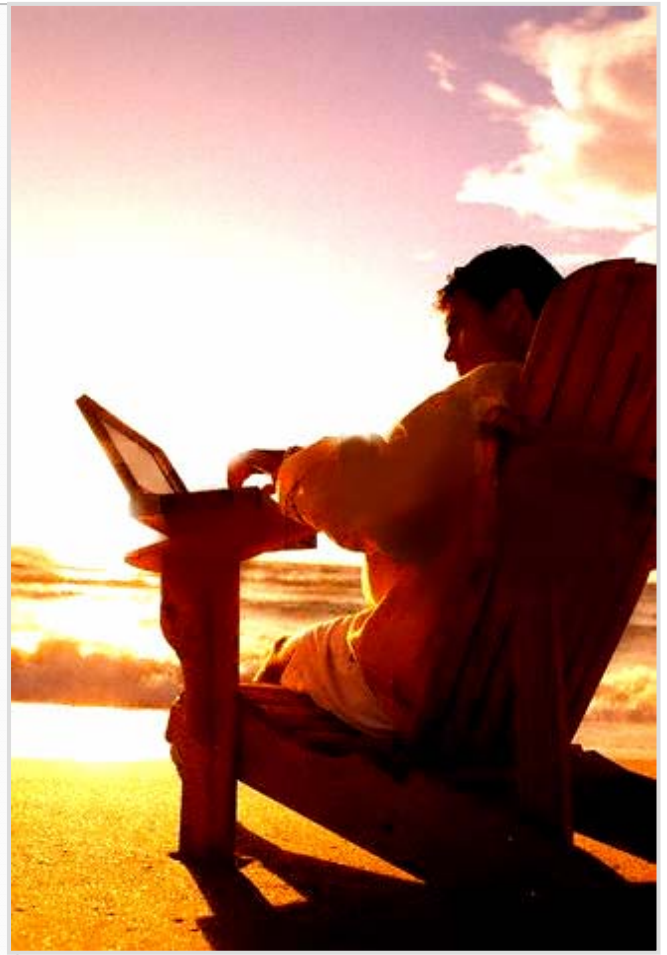


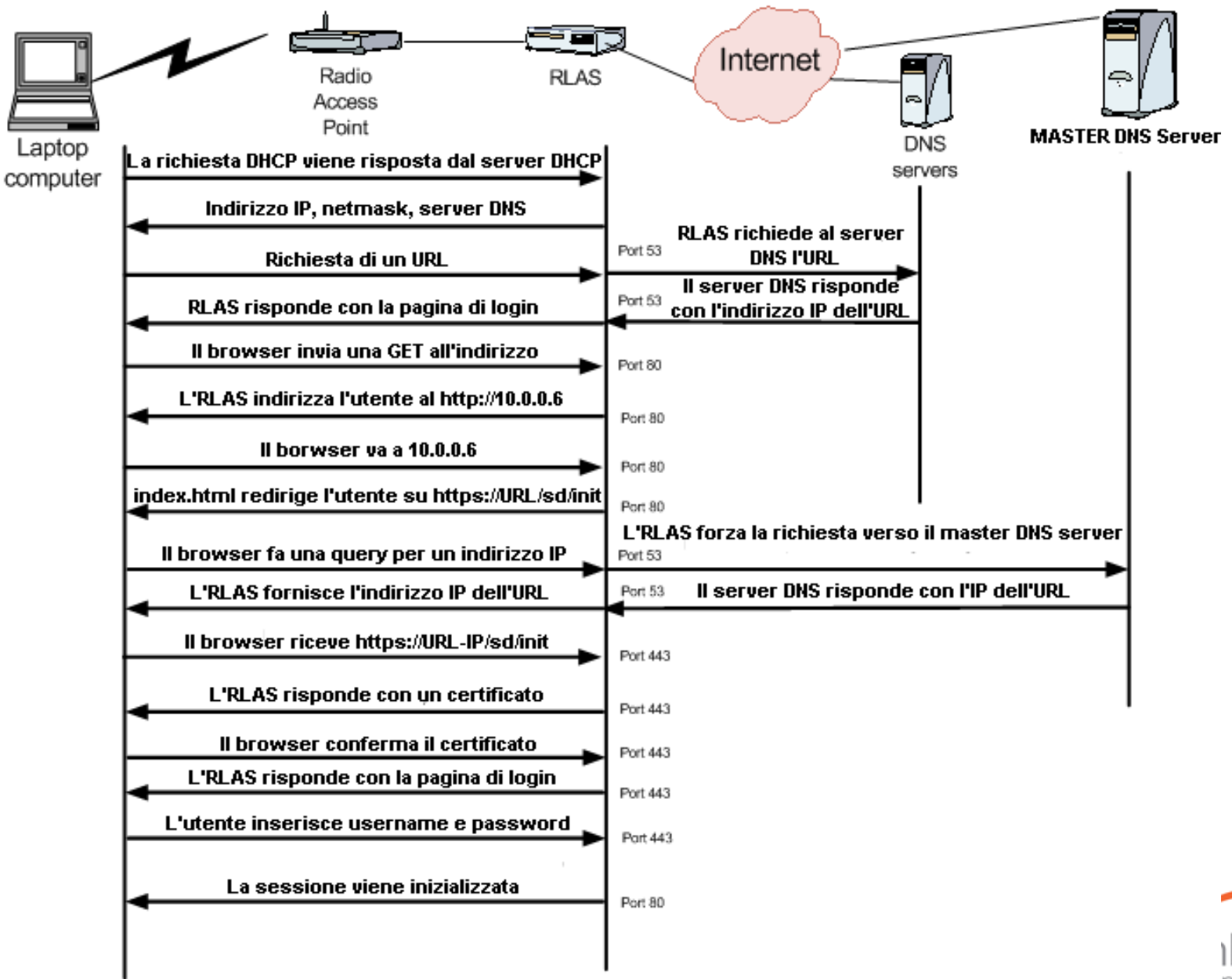
Call Detail Recording

Nelle telecomunicazioni, i CDR sono dei file contenenti informazioni sull'utilizzo di un sistema da parte di uno o più utenti.

```
C;lx1day03987;;mbit_visp;P000000091;SSI0000110;20051228060003;200512281445
56;;;346427597;15294686;15642961761760759821;2;4;15;SSI0000110;;;217.22.24
6.216;217.22.246.216;;BW_nordovest;excelsiorBG;
```

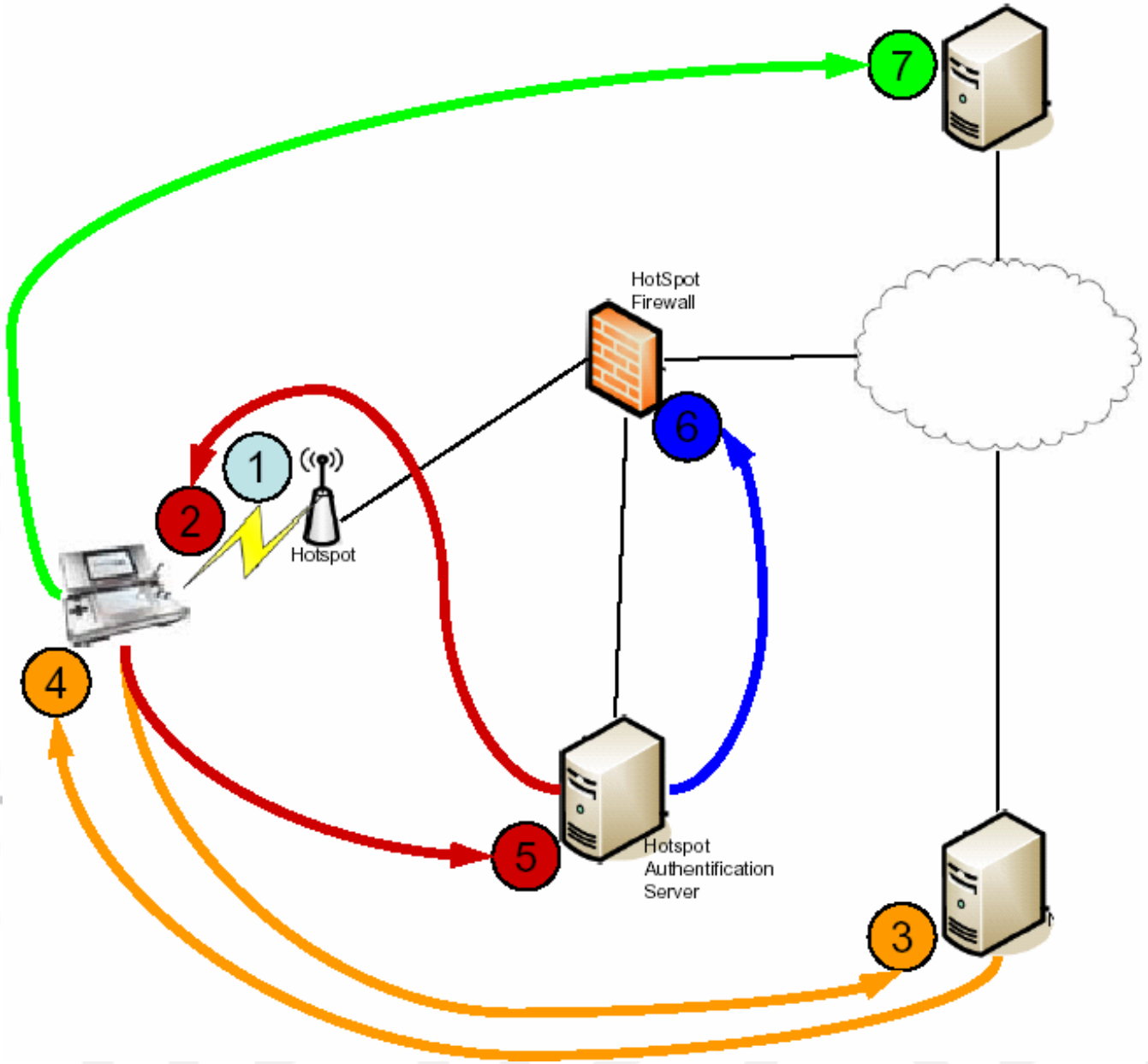
I CDR sono generati da un AMA (Automatic Message Accounting) e processati da un OSS (Operations Support System).




Laptop computer
Radio Access Point
RLAS
Internet
DNS servers
MASTER DNS Server
La richiesta DHCP viene risposta dal server DHCP
Indirizzo IP, netmask, server DNS
Richiesta di un URL
Port 53
RLAS richiede al server DNS l'URL
RLAS risponde con la pagina di login
Port 53
Il server DNS risponde con l'indirizzo IP dell'URL
Il browser invia una GET all'indirizzo
Port 80
L'RLAS indirizza l'utente al http://10.0.0.6
Port 80
Il borwser va a 10.0.0.6
Port 80
index.html redirige l'utente su https://URL/sd/init
Port 80
L'RLAS forza la richiesta verso il master DNS server
Il browser fa una query per un indirizzo IP
Port 53
L'RLAS fornisce l'indirizzo IP dell'URL
Port 53
Il server DNS risponde con l'IP dell'URL
Il browser riceve https://URL-IP/sd/init
Port 443
L'RLAS risponde con un certificato
Port 443
Il browser conferma il certificato
Port 443
L'RLAS risponde con la pagina di login
Port 443
L'utente inserisce username e password
Port 443
La sessione viene inizializzata
Port 80

La WECA ha distribuito un documento denominato “Best current practice”, ovvero una sorta di manuale con delle common actions da seguire al fine di standardizzare la customer experience in tutto il mondo.

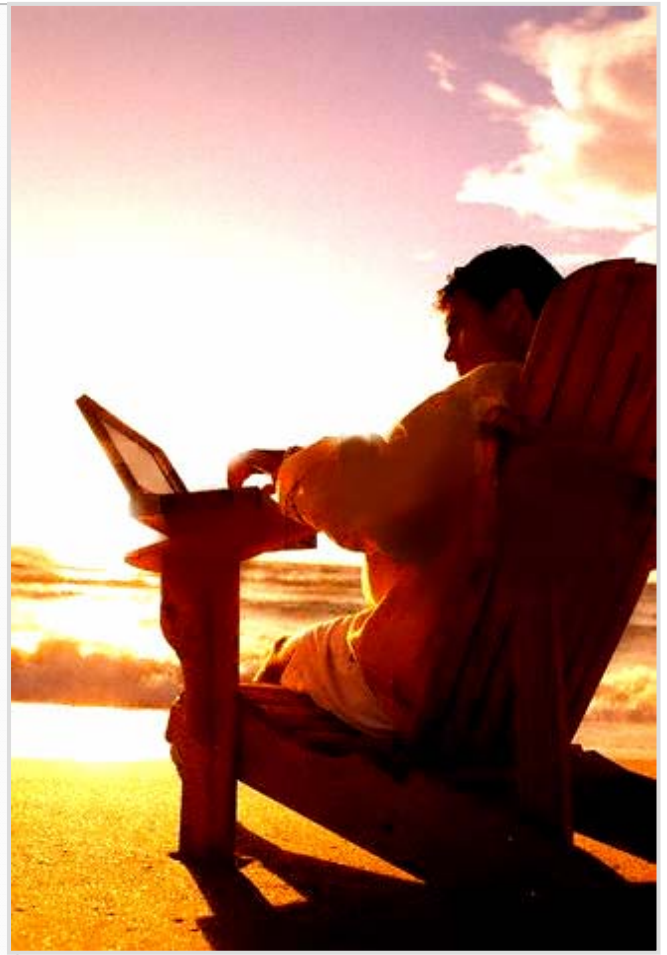
- Codice XML
- Attributi XML
- WISPr attributes
- SmartClient login

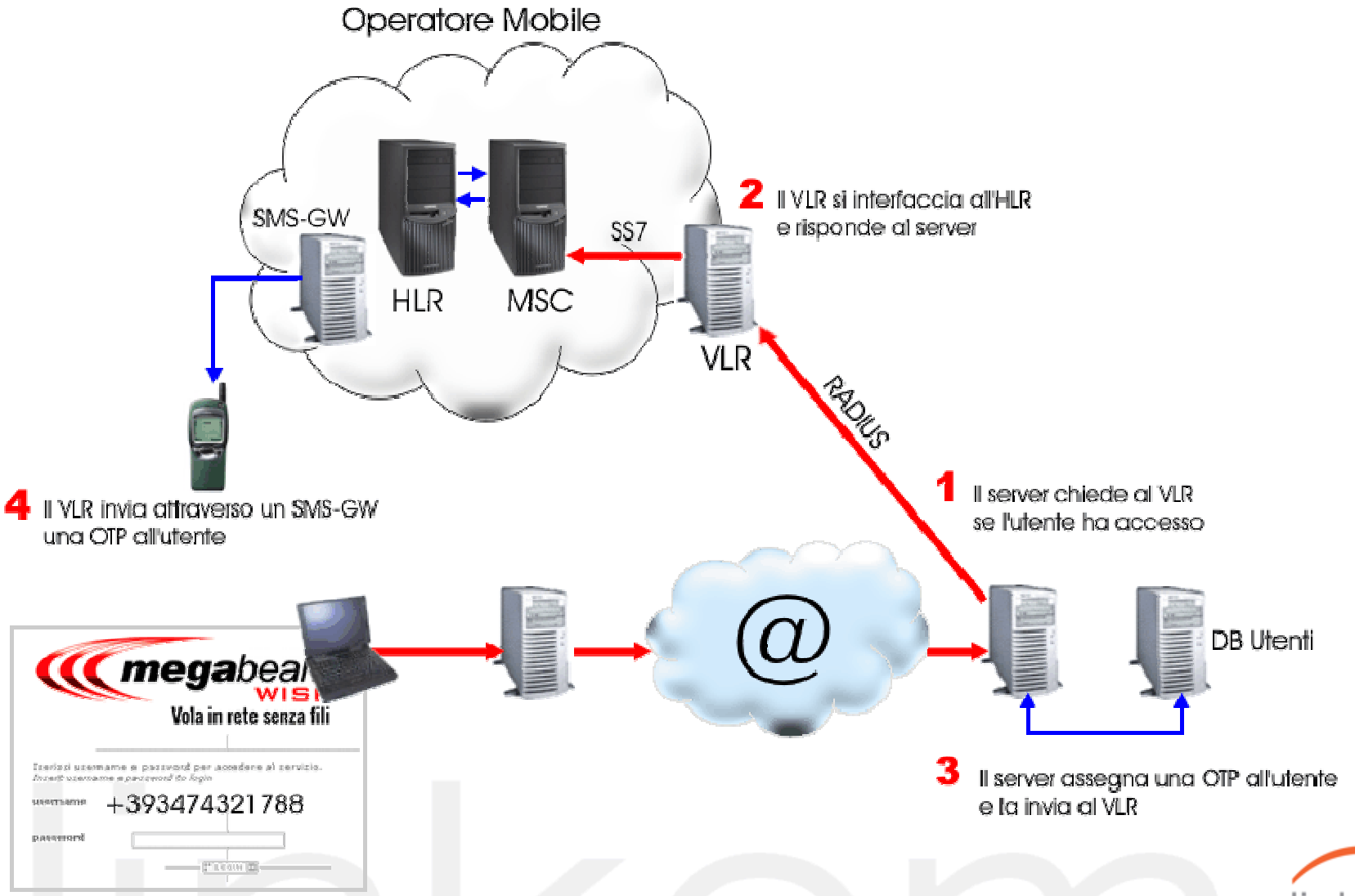


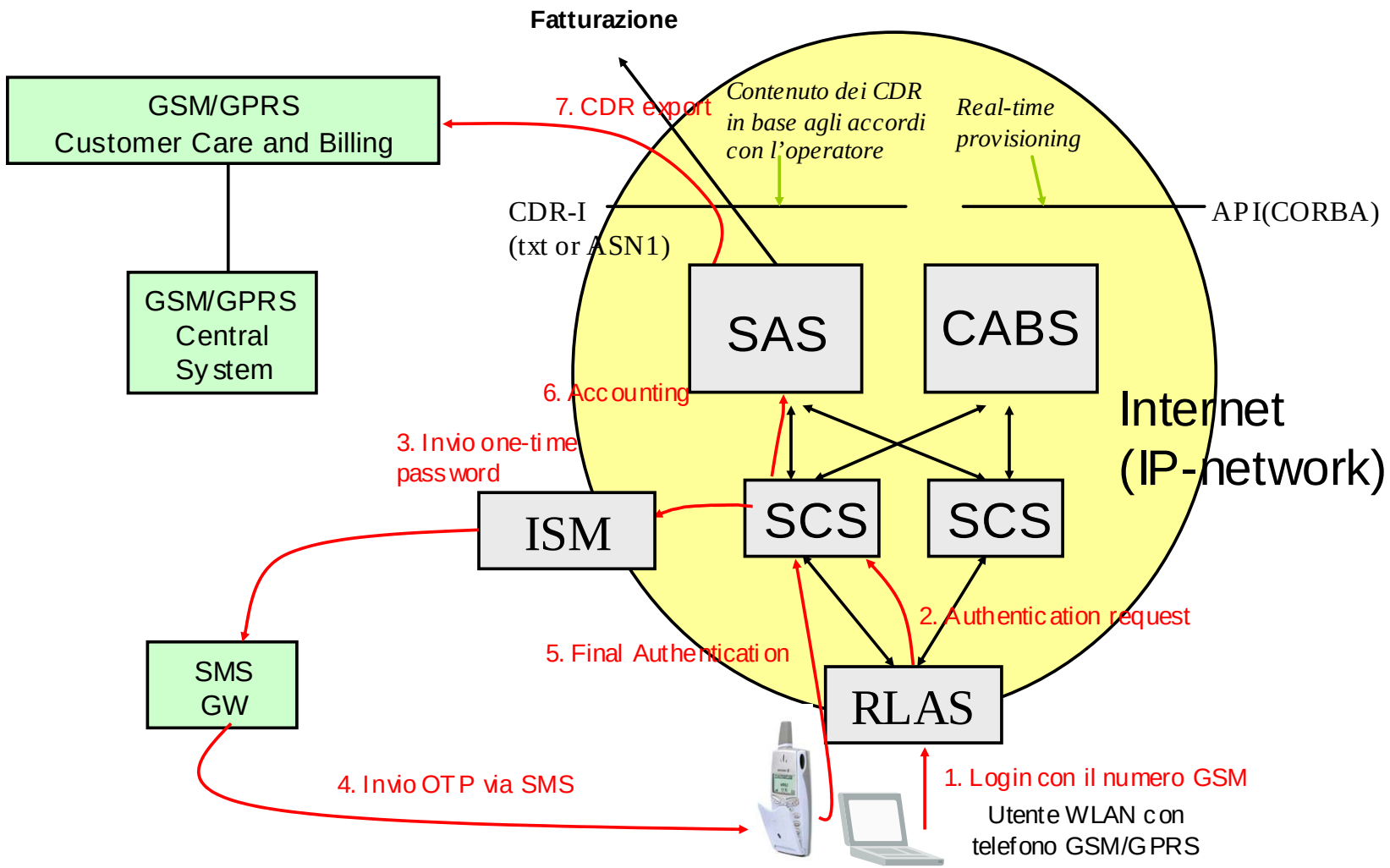
1.) Assegnazione indirizzo IP
2.) L'AS forza la pagina di login con i tag XML utilizzati dallo smart client per autenticarsi.
3.) Lo smart client invia i tag ad un server remoto.
4.) Il server remoto invia le informazioni per l'accesso al client.
5.) Il client invia le informazionidi accesso allo script dell'AS.
6.) L'AS verifica via RADIUS le credenziali di accesso.
7.) Se OK il client è libero di navigare.

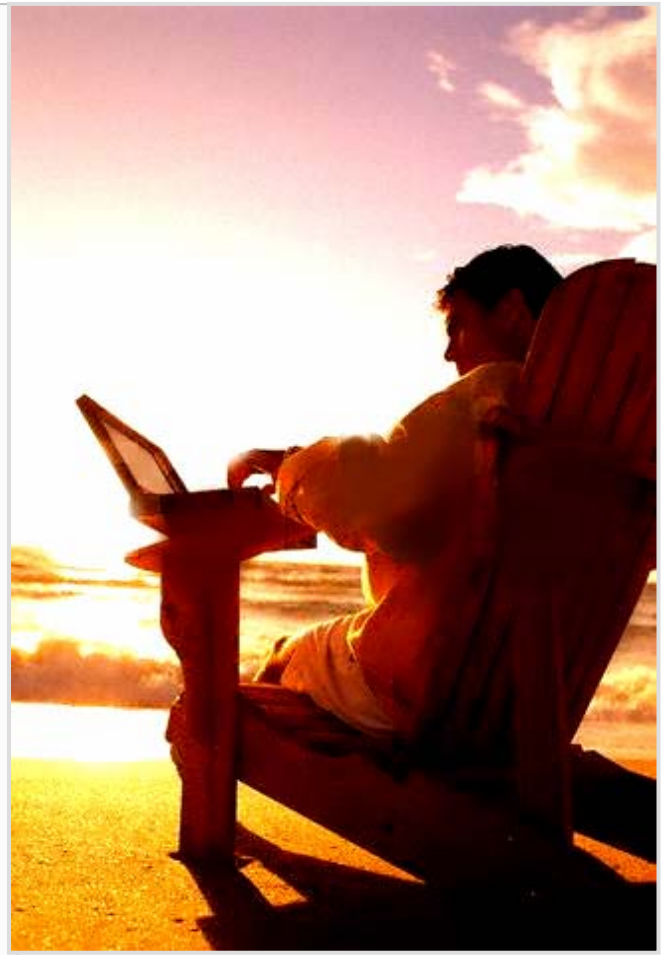
```
Connection: Keep-Alive
Cookie:
PREF=ID=cda45c335e7e4fb7:TM=1129377151:LM=1132312479:IG=2:S=9d8PTFWfNgiz4t_d

HTTP/1.1 302 Found
Date: Fri, 18 Nov 2005 11:42:46 GMT
Server: Apache
Location: https://login.linkem.com/sd/init?scheme=http&host=www.google.it&path=%2f
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

<!--

<?xml version="1.0" encoding="utf-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://login.linkem.com/smaccd/gis/WISPAccessGatew
ayParam.xsd">

  <Redirect>
    <AccessProcedure>1.0</AccessProcedure>
    <AccessLocation>SomeLocationId</AccessLocation>
    <LocationName>SomeLocationName</LocationName>
    <LoginURL>https://login.linkem.com/sd/gis_login</LoginURL>
    <AbortLoginURL>https://login.linkem.com/sd/gis_abort_login</AbortLoginURL>
    <MessageType>100</MessageType>
    <ResponseCode>0</ResponseCode>
  </Redirect>
</WISPAccessGatewayParam>

-->
```

```
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="http://www.linkem.com/xml/WISPA
ccessGatewayParam.xsd">
<AuthenticationReply>
        <MessageType>120</MessageType>
        <ResponseCode>50</ResponseCode>
        <ReplyMessage>Autenticazione Eseguita</ReplyMessage>
        <LoginResultsURL></LoginResultsURL>
        <LogoffURL>http://www.linkem.com/sd/logout</LogoffURL>
</AuthenticationReply>
</WISPAccessGatewayParam>

-->
```







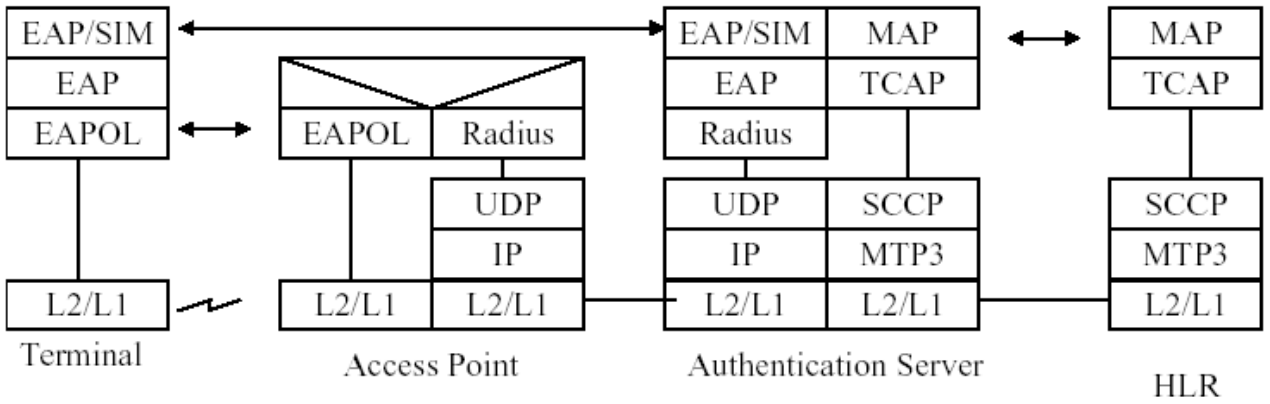


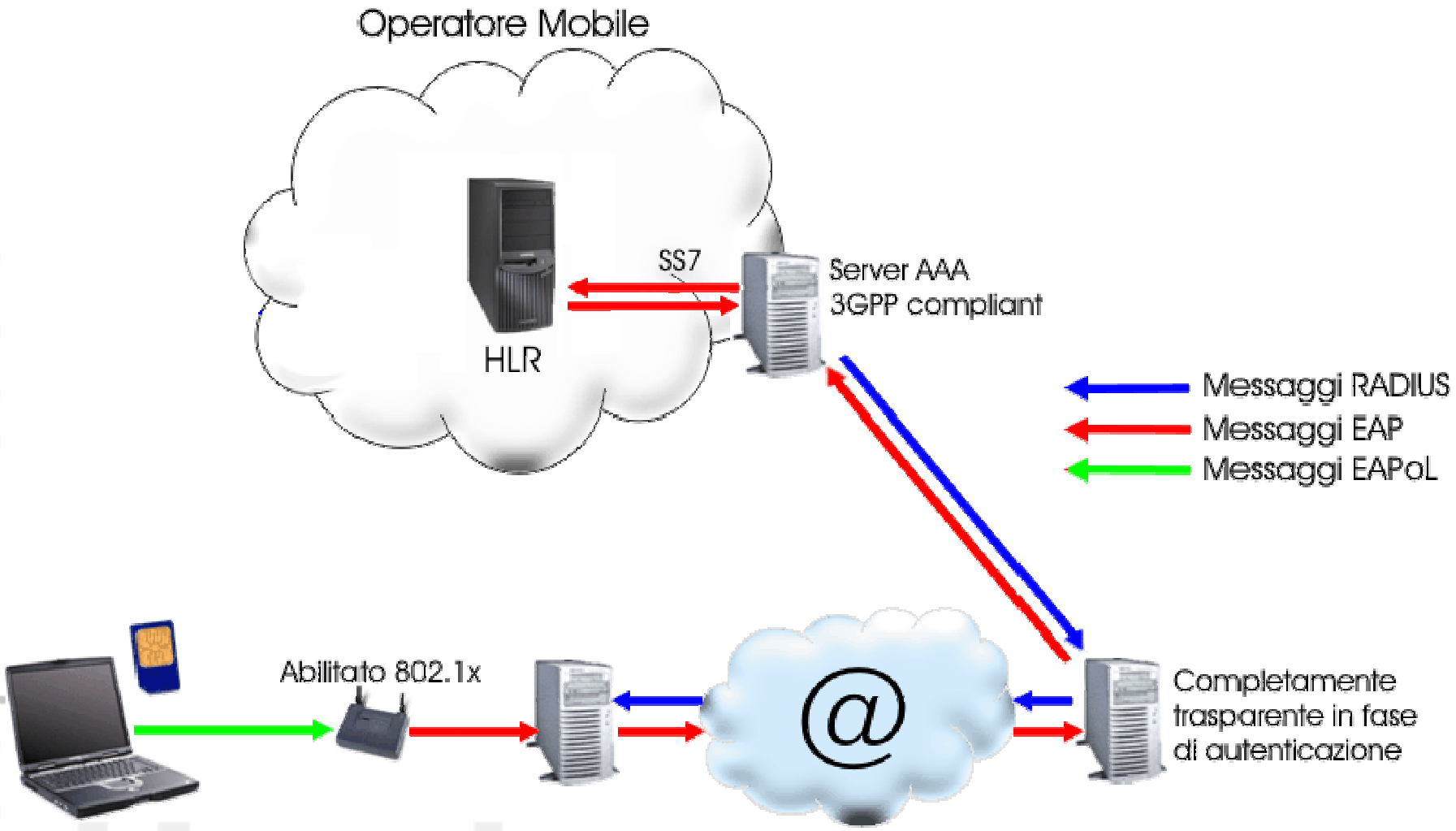
La SIM viene percepita come una tecnologia sicura sia dagli utenti che dagli operatori mobili ➔ possibilità di veicolare contenuti ad-hoc.

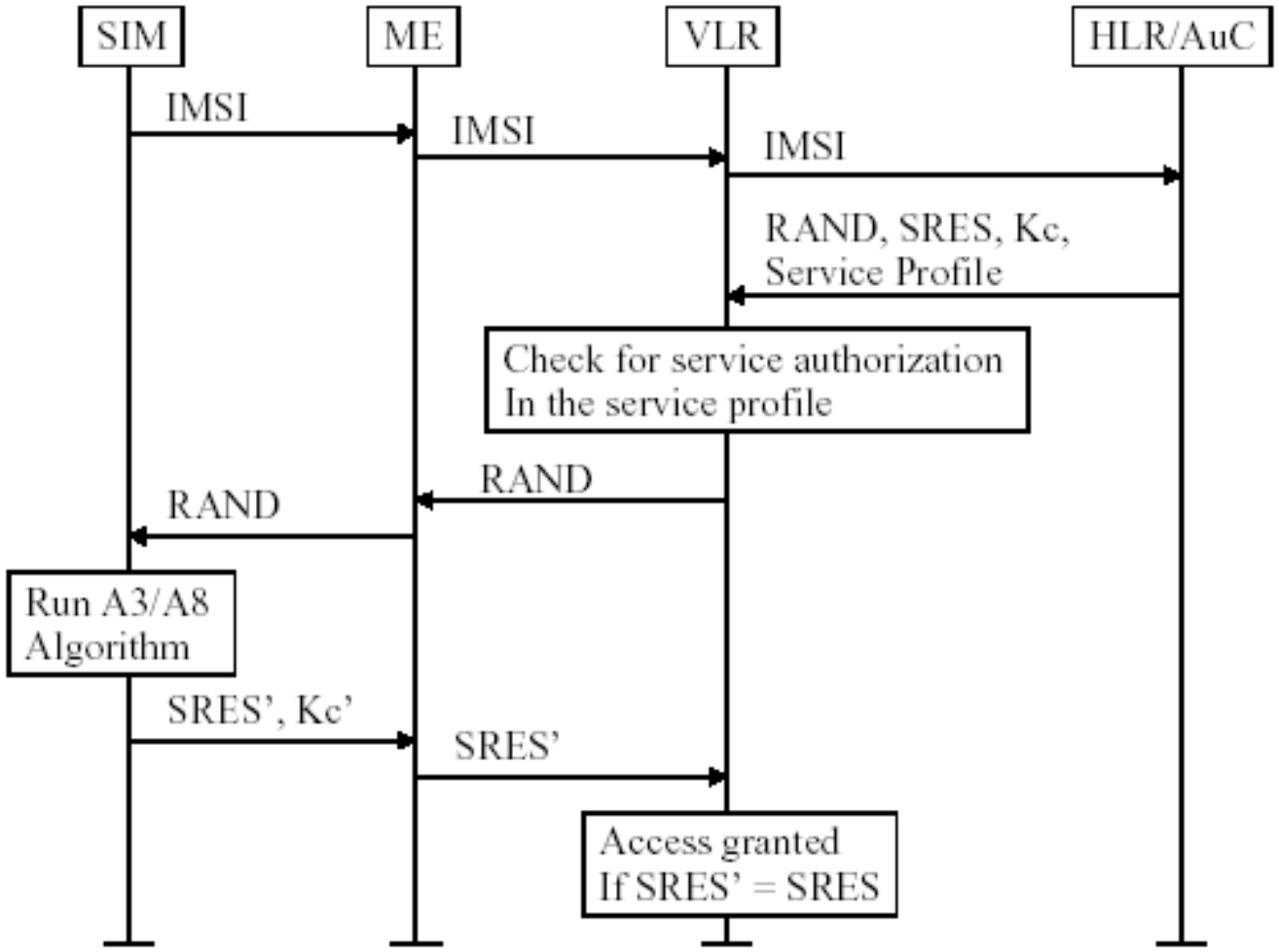
Il 3GPP si sta interessando al processo di interworking tra il mondo IP e quello mobile.

Utilizzo delle credenziali contenute nella SIM per autenticare l'utente alla wireless LAN (triplette GSM)

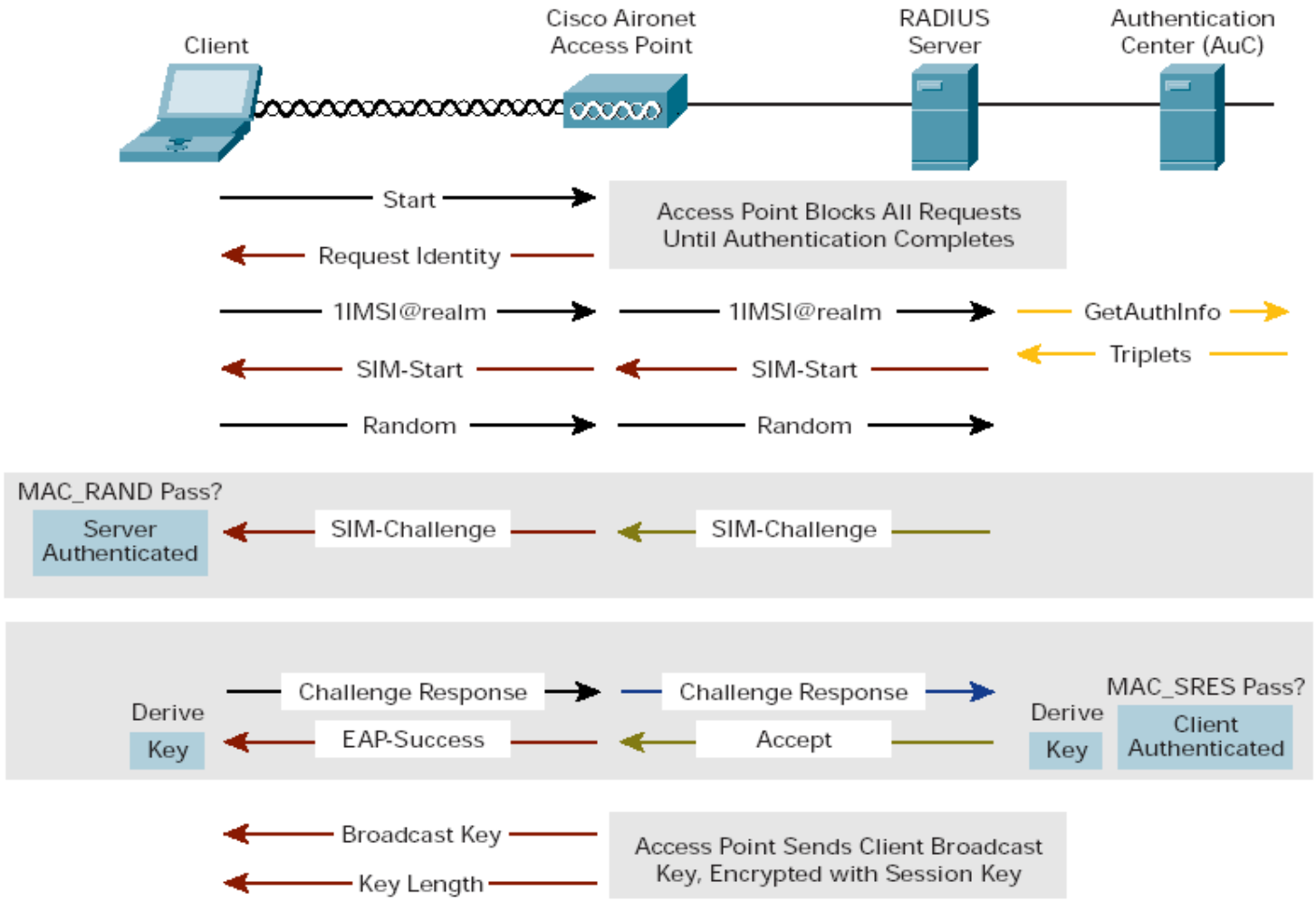
Necessità di interfacciarsi al network dell'operatore mediante un server di tipo AAA.







ARCHITETTURA LOCALE - EAP



keep in touch

VANTAGGI

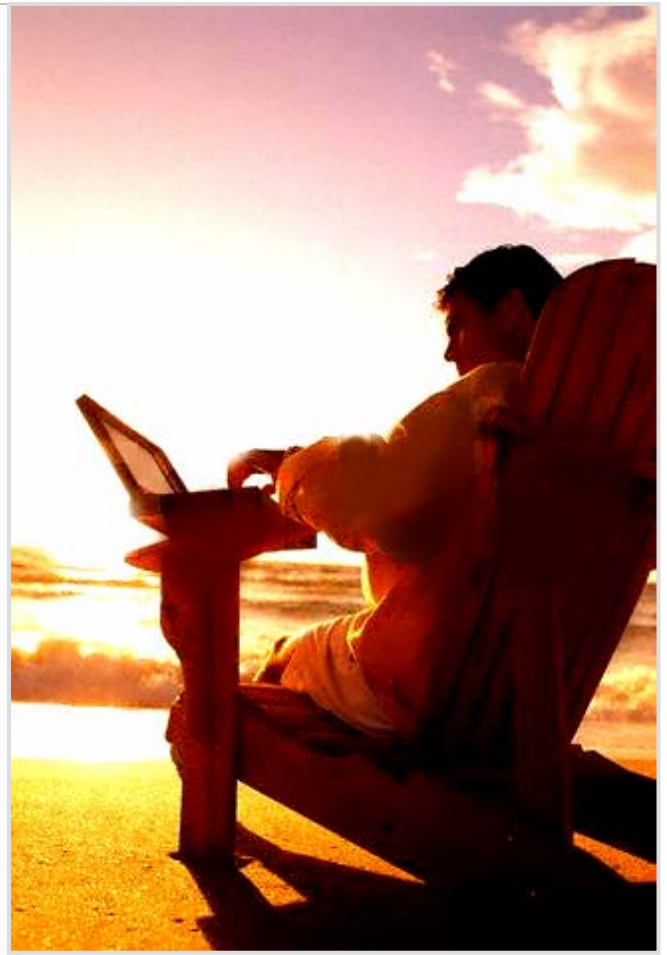
UTENTI

Percezione di un servizio unico, facile e immediatamente fruibile.
Unico bill
Integrazione tra WLAN e mobile ➔ aumento del bacino di utenza
Possibilità di veicolare contenuti mirati (profilazione)

OPERATORI

Aumento della sicurezza nelle location pubbliche
Futuro utilizzo degli algoritmi UMTS senza intaccare l'architettura
Gestione semplificata delle procedure di roaming

INDICE



keep in touch

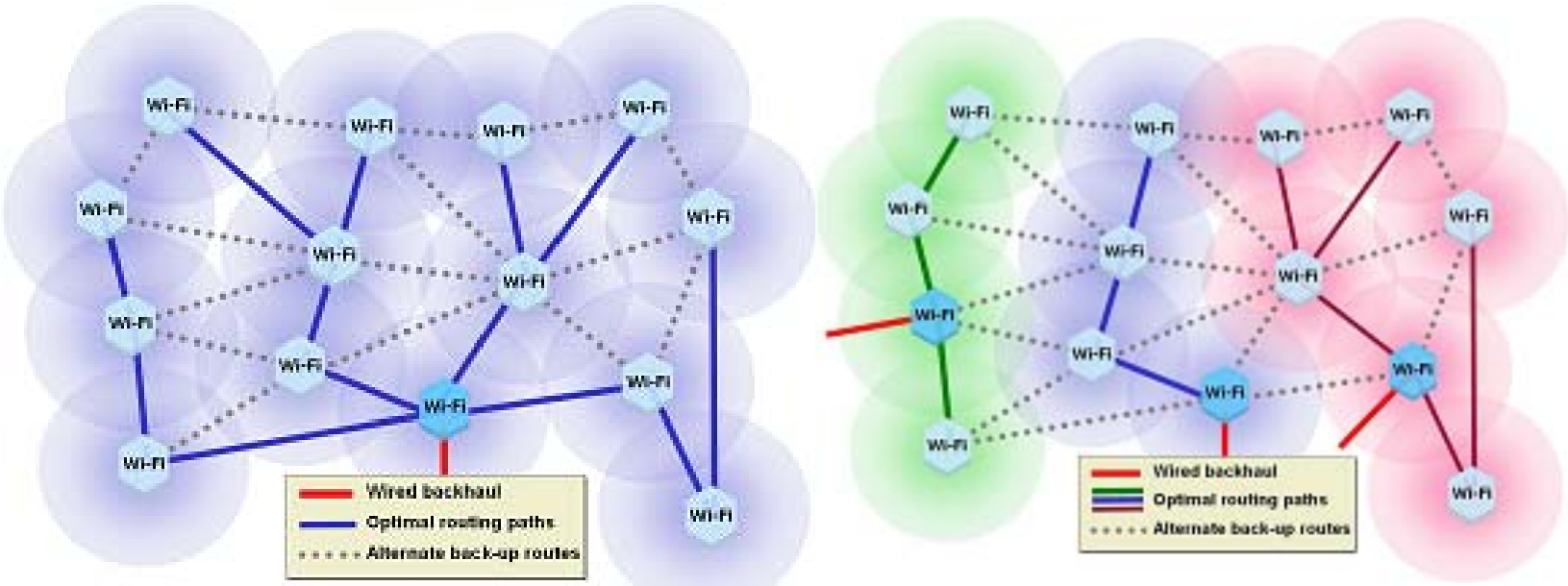
linkem
keep in touch

PROTOCOLLI

IEEE 802.11e - Miglioramento: Gestione della qualità del servizio.
IEEE 802.11F - Inter-Access Point Protocol (IAPP)
IEEE 802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) e Transmit Power Control (TPC) per compatibilità con l'Europa
IEEE 802.11i (ratified 24 giugno 2004) - Miglioramento della sicurezza
IEEE 802.11j - Estensione per il Giappone
IEEE 802.11k - Misurazione delle sorgenti radio
IEEE 802.11n - Aumento della banda disponibile
IEEE 802.11p - WAVE - Wireless Ability in Vehicular Environments (gestione per autoveicoli, ambulanze, ecc...)
IEEE 802.11r - Roaming rapido
IEEE 802.11s - Gestione della topologia della rete
IEEE 802.11T - Gestione e Test
IEEE 802.11u - Connessione con reti non 802 , tipo le reti cellulari.
IEEE 802.11v - Gestione delle reti wireless

- **Integrazione tra rete WiFi e rete GSM/UMTS**
- **Handover "trasparente" tra le due reti (3GPP)**
- **Sicurezza implementata tramite l'AES**

- **Reti Mesh**



- Handover tra rete GSM/UMTS e rete WiFi
- Protocolli di routing per mesh networks
- Studio e configurazione di Diameter
- Replication di un accounting server RADIUS
- Quality Of Service su WiFi
- VoWLAN

linkem
keep in touch

E' UN BRAND DI MEGABEAM ITALIA SPA

Contatti

Megabeam Italia Spa

Sito: www.linkem.com

Email: maurizio.martinoli@linkem.com

MEGABEAM ITALIA SPA
Viale Città D'Europa 681 - 00144 ROMA
TEL +39 06 52 05 907
FAX +39 06 52 98 307

www.linkem.com