9° Workshop tecnico GARR - Roma 15-18 giugno 2009

AAA e wireless: scelte implementative, gestione e monitoraggio

Paolo Gaiardelli & Stefano Moroni

Università degli studi di Milano Bicocca

Contesto realizzativo

- ***Elevato numero di utenti***
  40/50.000 tra studenti e personale

- ***Elevato numero di sedi universitarie***
  22 sedi in Lombardia

- ***Elevato numero di apparati di rete coinvolti***
  400 apparati di accesso, 400 AP, 6 WLAN controller

- ***Elevato grado di eterogeneità di utenza***
  diverso utilizzo della rete

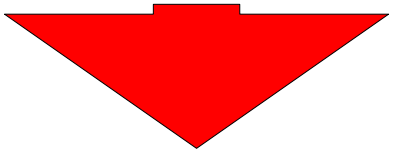
- ***Mobilità e nomadismo***
  di utenti unimib e utenti roaming

Vincoli e requisiti normativi

D. Lgs. n. 196/2003
Codice unico in materia di protezione dei dati personali - DPSS

L. n. 155/2005
Conversione in legge del D.L. n. 144/05 recante misure urgenti per il contrasto del terrorismo internazionale

Acceptable Use Policy del GARR
"Tutti gli utenti a cui vengono forniti accessi alla rete devono essere riconosciuti e identificabili"



Obbligo di identificare con certezza l'utente che ha accesso alla rete (associazione tra indirizzo IP utilizzato e utente).
Obbligo di mantenere per un certo periodo questi dati.
Obbligo di attuare tutte le misure di sicurezza in linea con gli sviluppi tecnologici per l'implementazione delle politiche.

Vincoli e requisiti tecnici

- **Dimensionamento**
  Elevato numero di accessi concorrenti → Alta disponibilità e scalabilità su grandi numeri

- **Tipologie di connessione**
  Utenti strutturati e ospiti → Elasticità negli accessi

- **Sicurezza nell'accesso** → Livello adeguato per ogni tipologia di accesso

- **Utenti "roaming"** → Garantire accesso utenti "Eduroam"

- **Protocolli e software** → Standard e "open source" (no dipendenza da vendor)

- **Compatibilità e portabilità** → Qualunque OS e connettività "clientless"

Tipologie di rete

Architettura centralizzata

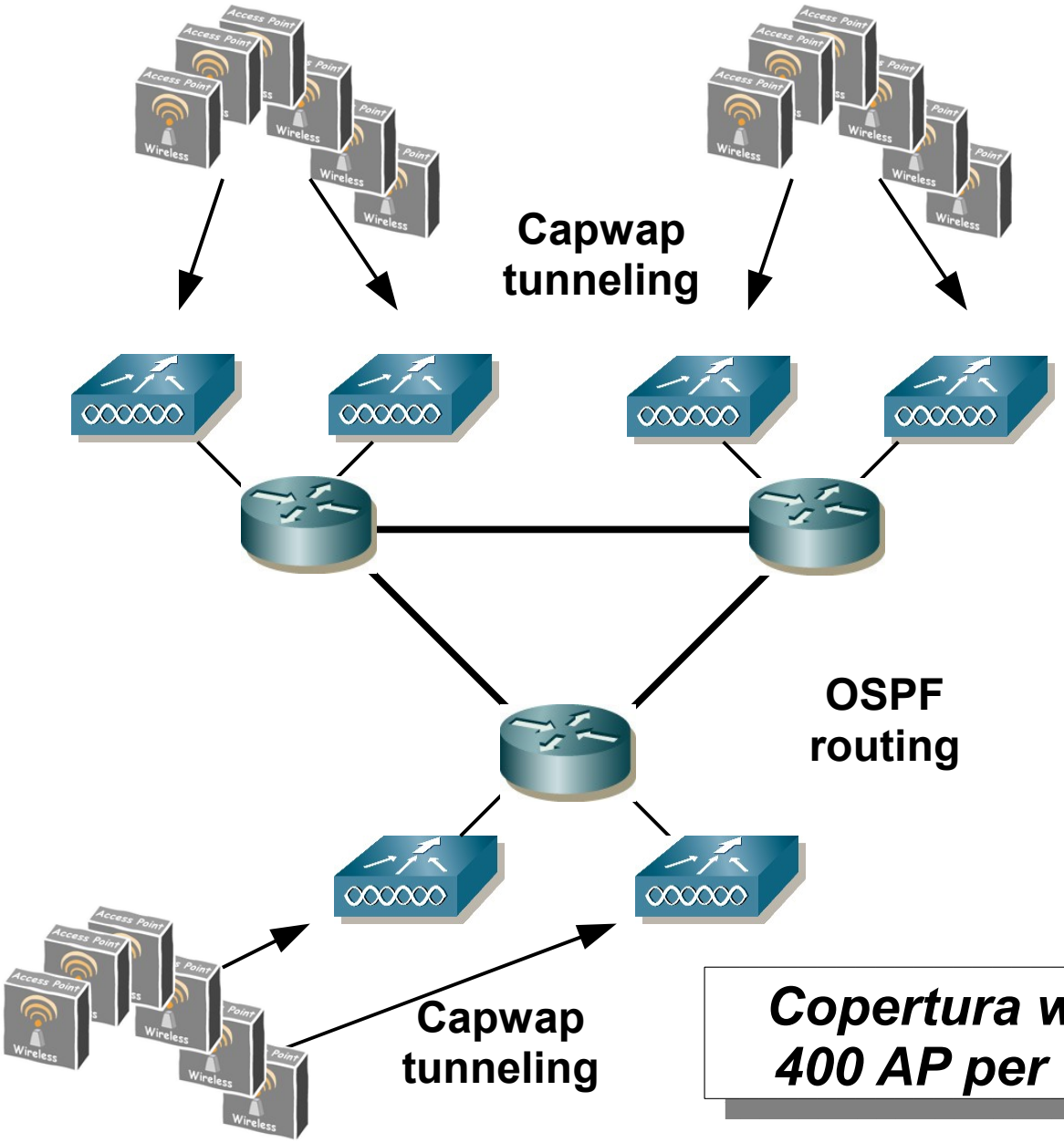
- *logica di accesso centralizzata su wireless controller con AP di tipo "thin" (solo chipset per cifratura)*
- *single point of policy enforcement*
- *roaming più semplice*
- *rogue AP detection, gestione automatica RF*
- *scalabilità in funzione del numero di controller*

Architettura distribuita

- *logica di accesso implementata sui "thick" AP*
- *policy enforcement puntuale*
- *roaming più complesso*
- *scalabilità in funzione del numero di AP*

Si è optato per una architettura centralizzata privilegiando gli aspetti di gestione e monitoraggio rispetto all'inconveniente di un instradamento non sempre ottimale all'interno di tale modello (problema sedi remote)

Rete Wireless Unimib



Alta disponibilità:
ogni coppia di WLAN Controller è collegata a uno dei nodi di core backbone

Gli Access Point sono concentrati sui controller tramite tunnel a layer3 su protocollo CaPWAP (RFC 5415)

Copertura wireless completa dell'Ateneo
400 AP per una superficie di 230.000 mq

Tecnologie di accesso alle reti wireless

Captive Portal (https con certificato server)

- semplice da implementare
- clientless e indipendenza da OS
- no cifratura canale wireless

VPN (Virtual Private Network)

- cifratura canale
- necessita distribuzione client configurato
- non scalabile

Standard IEEE 802.11i

- diversi livelli di cifratura canale wireless
- supportato nativamente in tutte le piattaforme
- fornisce trasporto per protocolli di AAA
- 802.1X è diffuso anche per accesso wired (unico backend per accessi alla rete)

Soluzioni adottate

Protocolli di accesso

Standard IEEE 802.11i

- 802.1X implementato su tutti gli apparati di rete e già utilizzato per accessi wired
- AAI già in produzione

Autenticazione, Autorizzazione, Accounting

Protocollo RADIUS

- Standard IETF RFC 2865 e successive integrazioni
- Protocollo di AAA compatibile con 802.1X e LDAP

Repository delle identità degli utenti

Protocollo LDAPv3

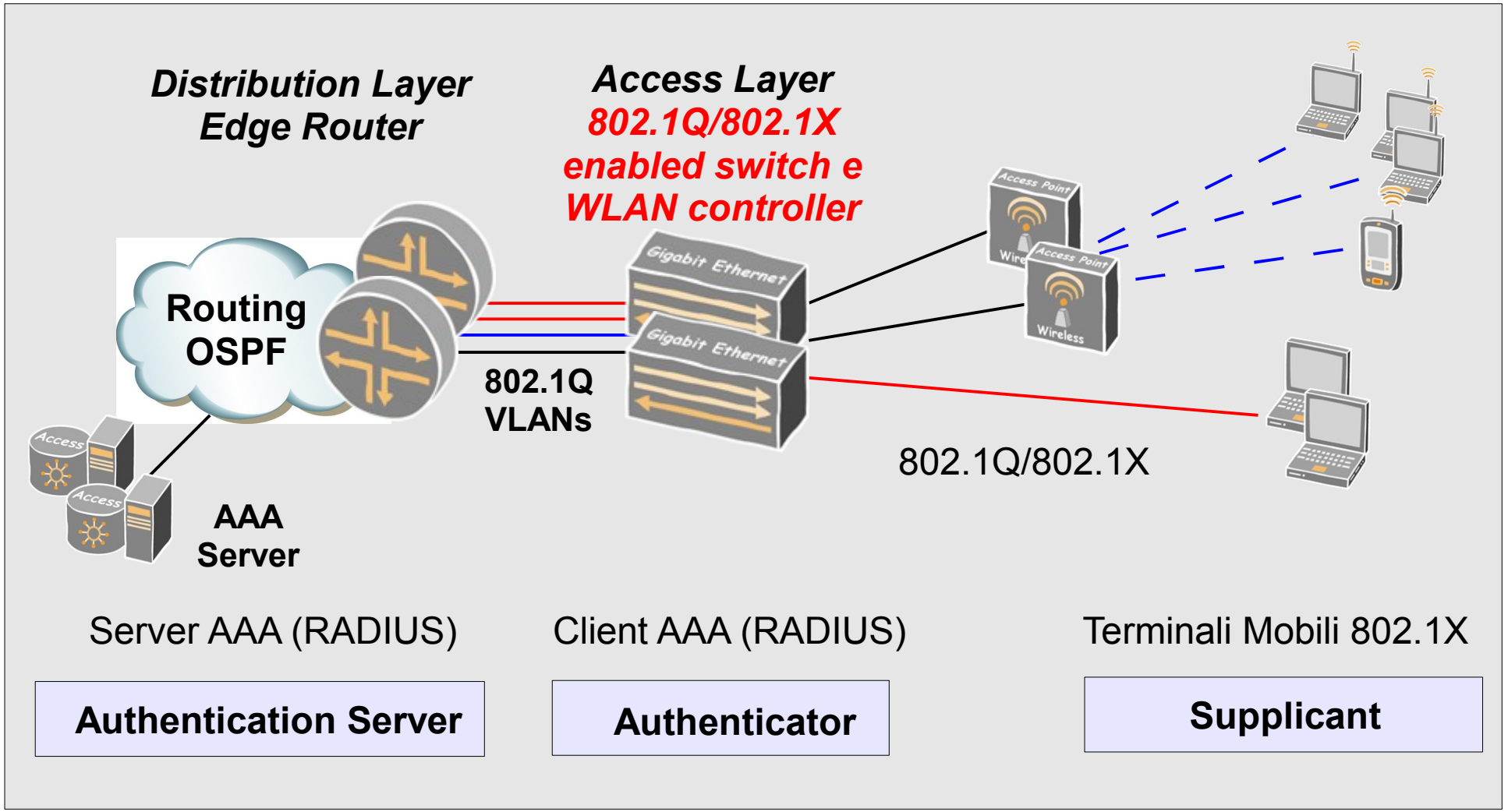
- Standard IETF RFC 2251 e successive integrazioni
- Protocollo di interrogazione per servizi di directory

Architettura 802.1X

Supplicant — *terminale che chiede l'accesso alla rete*

Authenticator — *apparato di rete al quale il supplicant si connette*

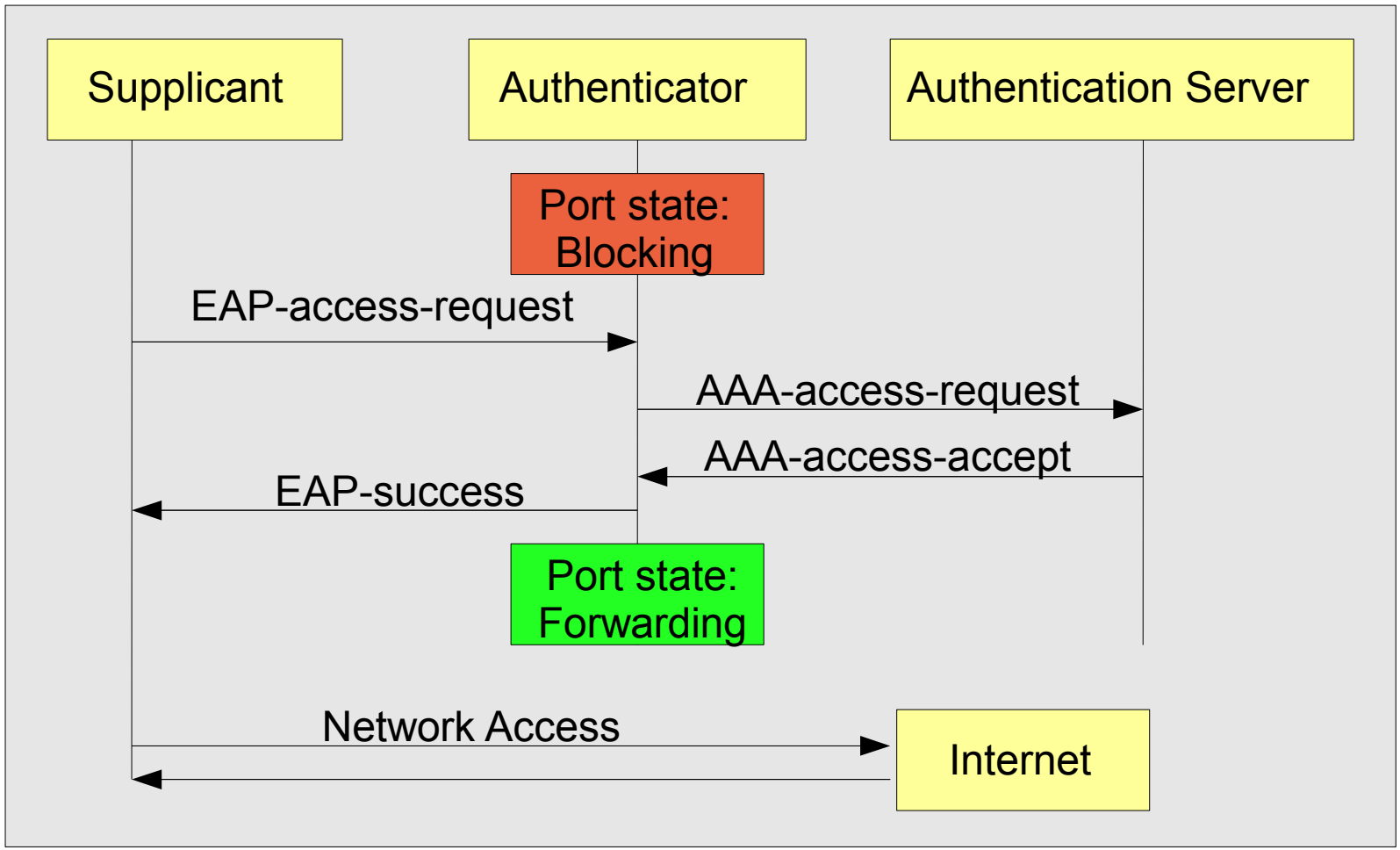
Authentication Server — *server di backend della logica di AAA*



Flusso 802.1X

1) *La porta di accesso è tenuta in stato di "blocking"*

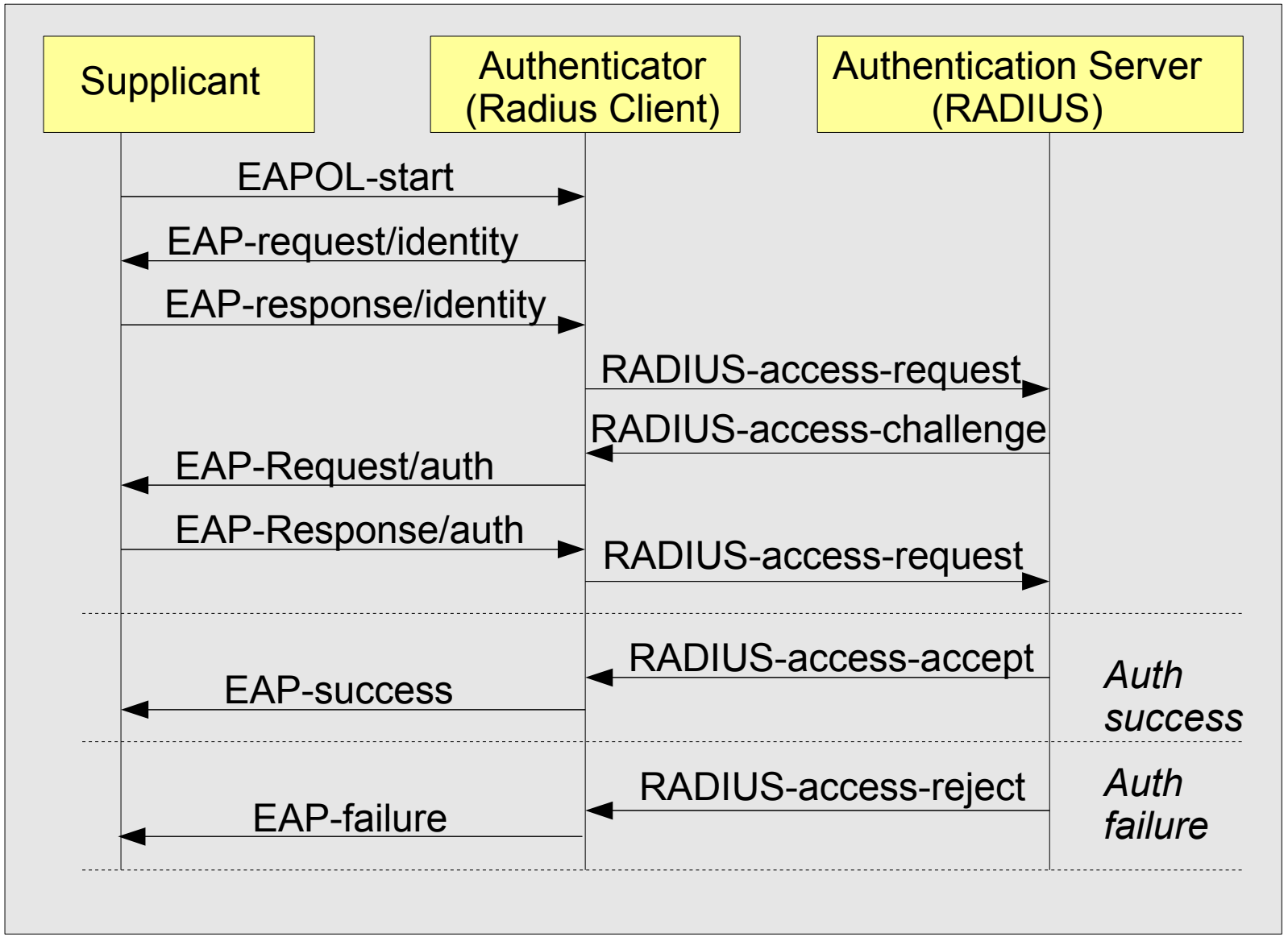
2) *L'Autenthicator riceve ed inoltra la richiesta di accesso del terminale utente all'Autentication server (fase di AA)*



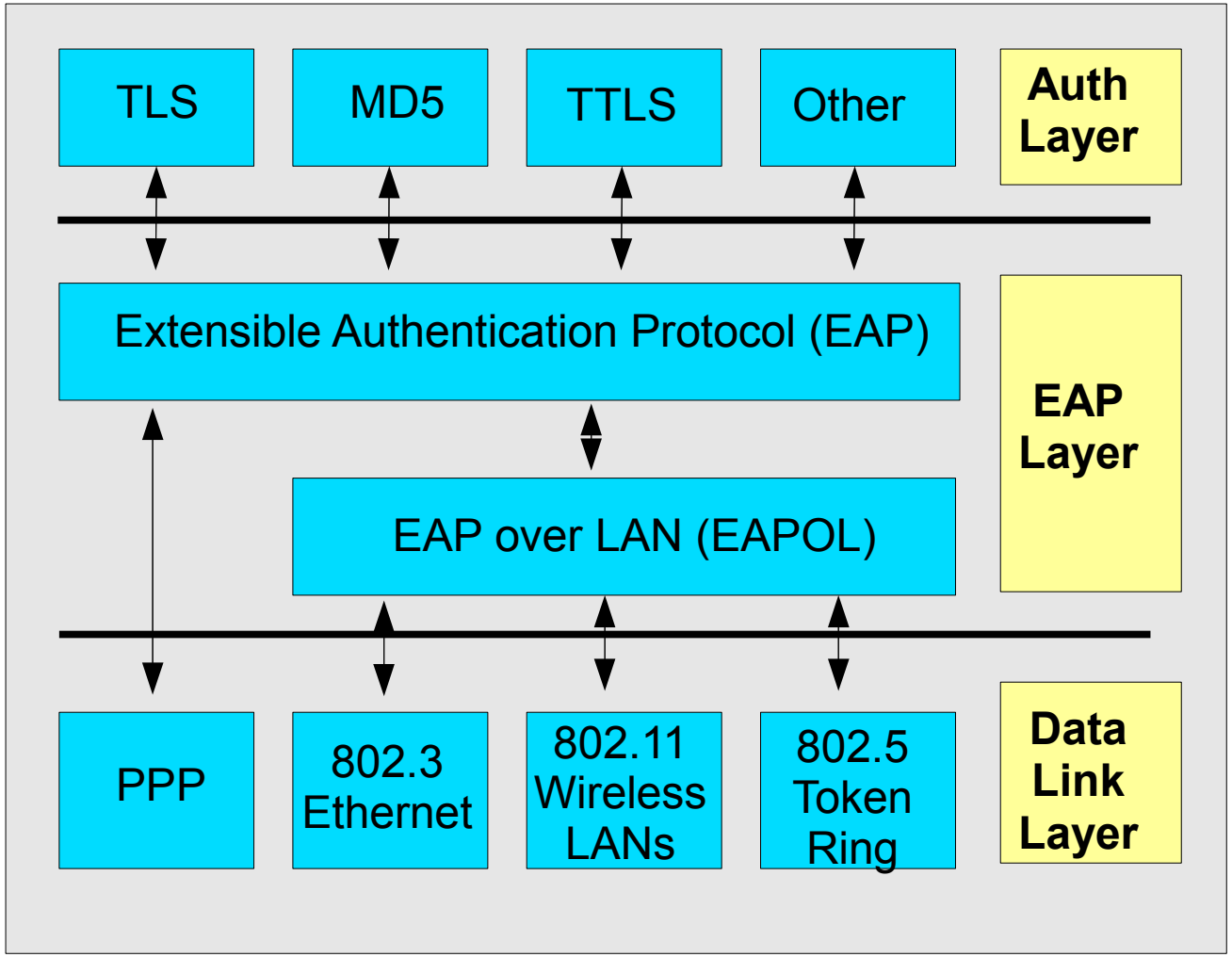
3) *Terminata la fase di AA: porta di accesso in"forwarding"*

Negoziazione 802.1X

Per l'autenticazione si basa sul protocollo EAP (RFC3748) tramite il quale si interfaccia con la logica di AAA



Scelta metodo di autenticazione EAP



EAP è un "framework" per l'autenticazione tra i nodi di rete - supporta diversi metodi di autenticazione basati su differenti schemi e algoritmi di cifratura.

Scelta metodo di autenticazione EAP

Per offrire una reale alternativa alla connessione cablata il livello di sicurezza offerto deve essere lo stesso

I metodi "sicuri" con diffusione accettabile sono EAP-TLS o EAP-TTLS/PEAP

EAP-TTLS e PEAP suscettibili a errore umano nella mancata verifica del certificato server (distrazione)

L'unico modo per evitare la compromissione delle credenziali che l'utente utilizza anche per altri scopi è non utilizzarle:

EAP-TLS

Alternativa: usare altre credenziali per l'accesso wireless

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Le credenziali utente (username e password) nel directory server LDAP danno accesso a tutti i servizi applicativi di rete di Ateneo e ai dati personali degli utenti

L'intercettazione fraudolenta delle credenziali utente deve essere tecnicamente infattibile e il metodo da implementare deve minimizzare anche il possibile errore umano o di distrazione

Rischi: "man-in-the-middle", "replay attack", "eavesdropping"

Contromisure: Crittografia a chiave pubblica e riconoscimento sicuro degli "end point" del dialogo cifrato

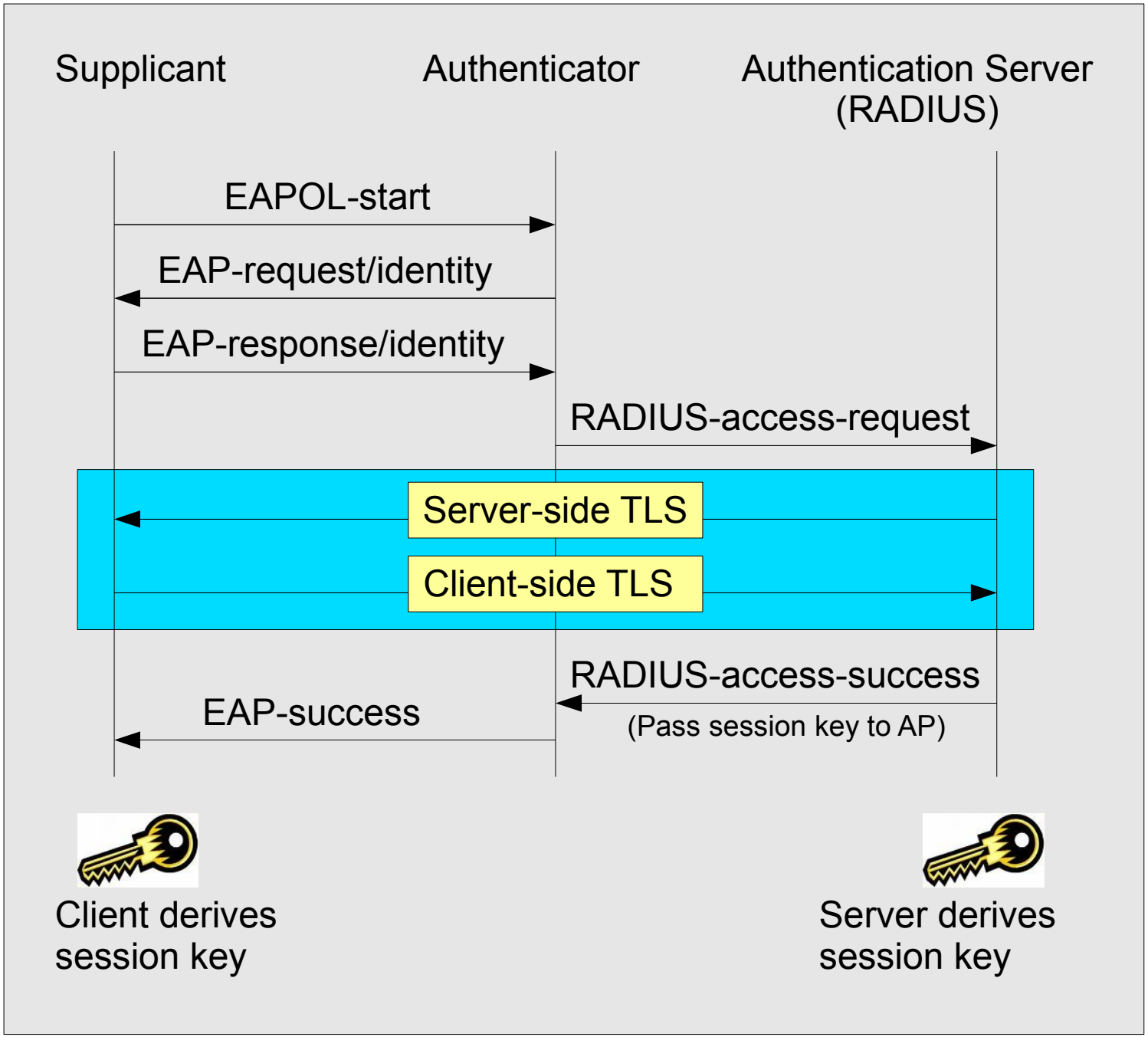
EAP-TLS

Mutua autenticazione tra client (supplicant) e server di autenticazione con certificati X.509.

Non necessita l'invio della password (minimizza errore umano)

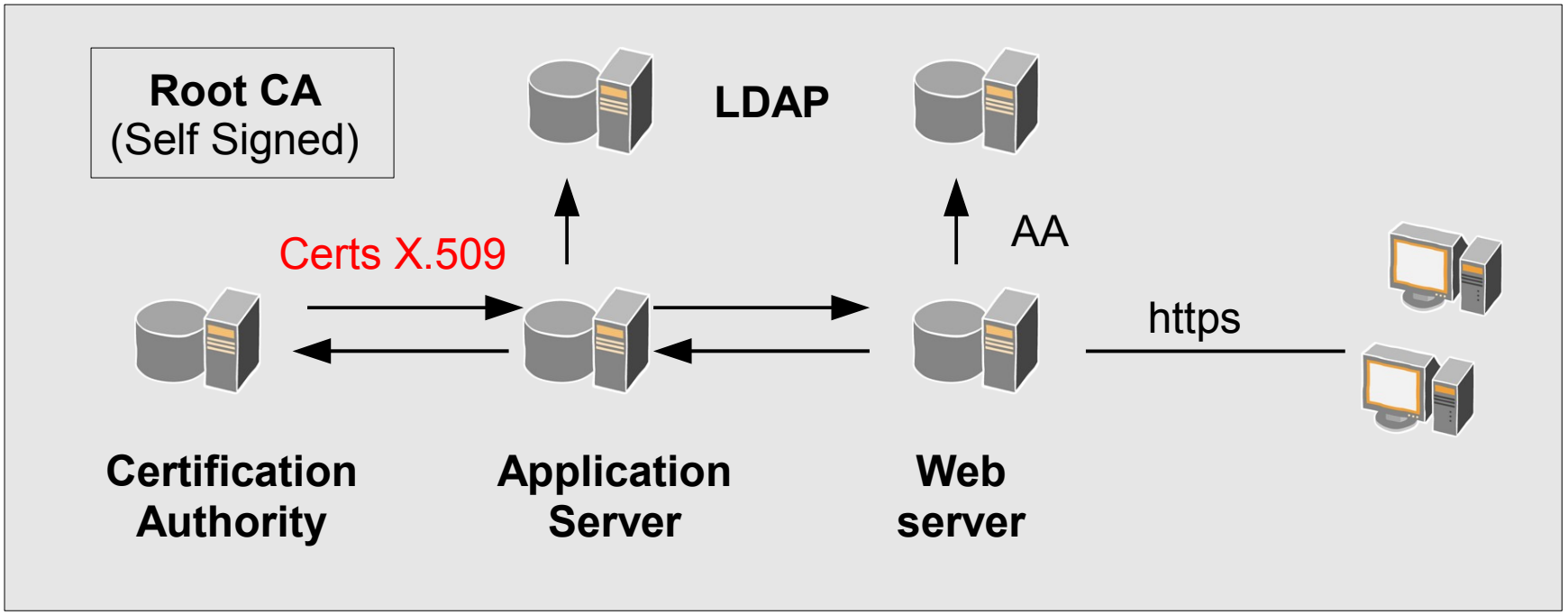
Controindicazione: Infrastruttura a Chiave Pubblica (PKI) per la generazione e distribuzione dei certificati X.509 per gli utenti

Inserimento dello strato TLS in EAP



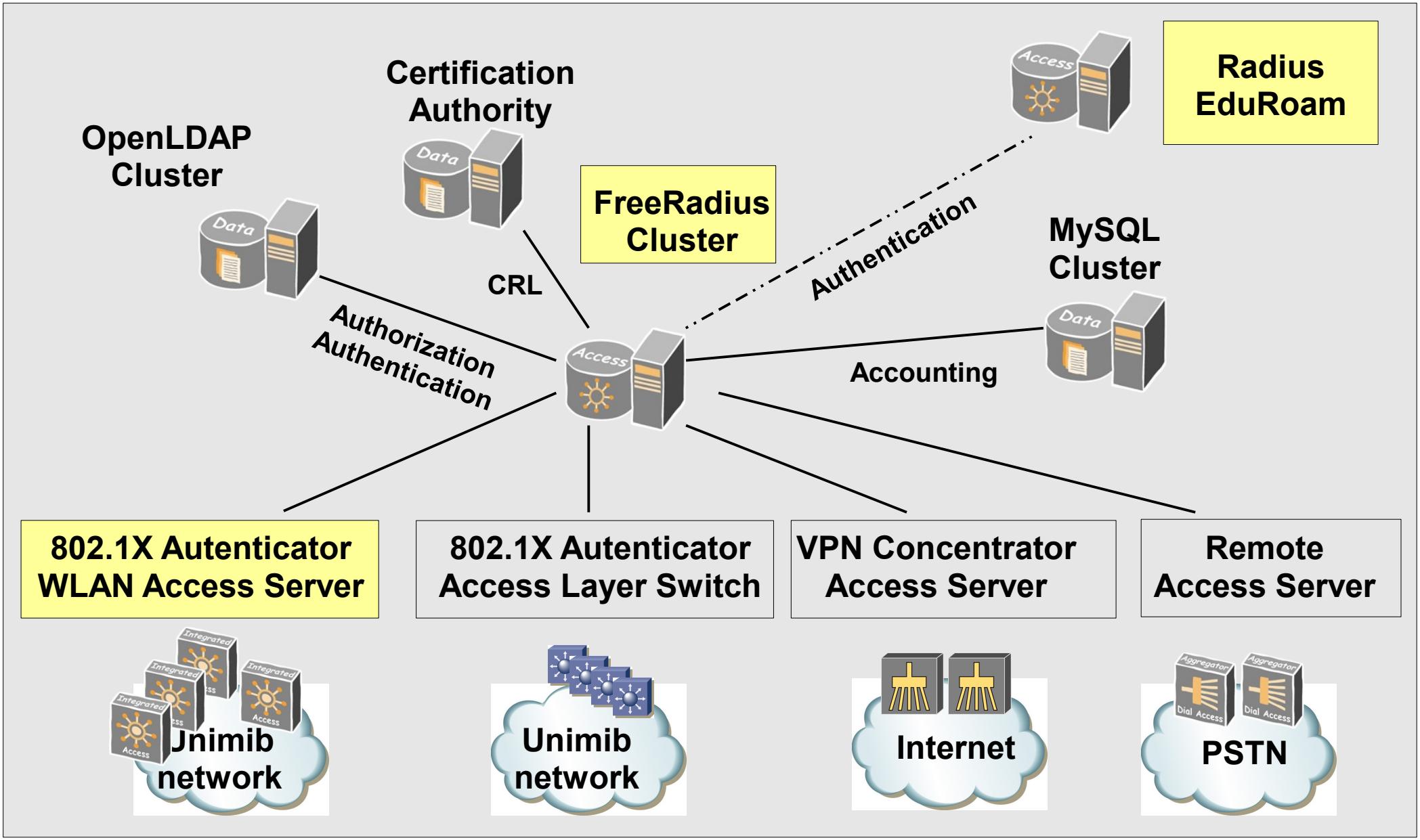
Infrastruttura a chiave pubblica

Per realizzare la PKI è stato necessario utilizzare una Certification Authority per la generazione dei certificati e costruire la parte di "Registration Authority".



E' stata sviluppata anche una procedura web che si interfaccia con la RA per la generazione online e il download dei certificati

Schema architettura e AAI



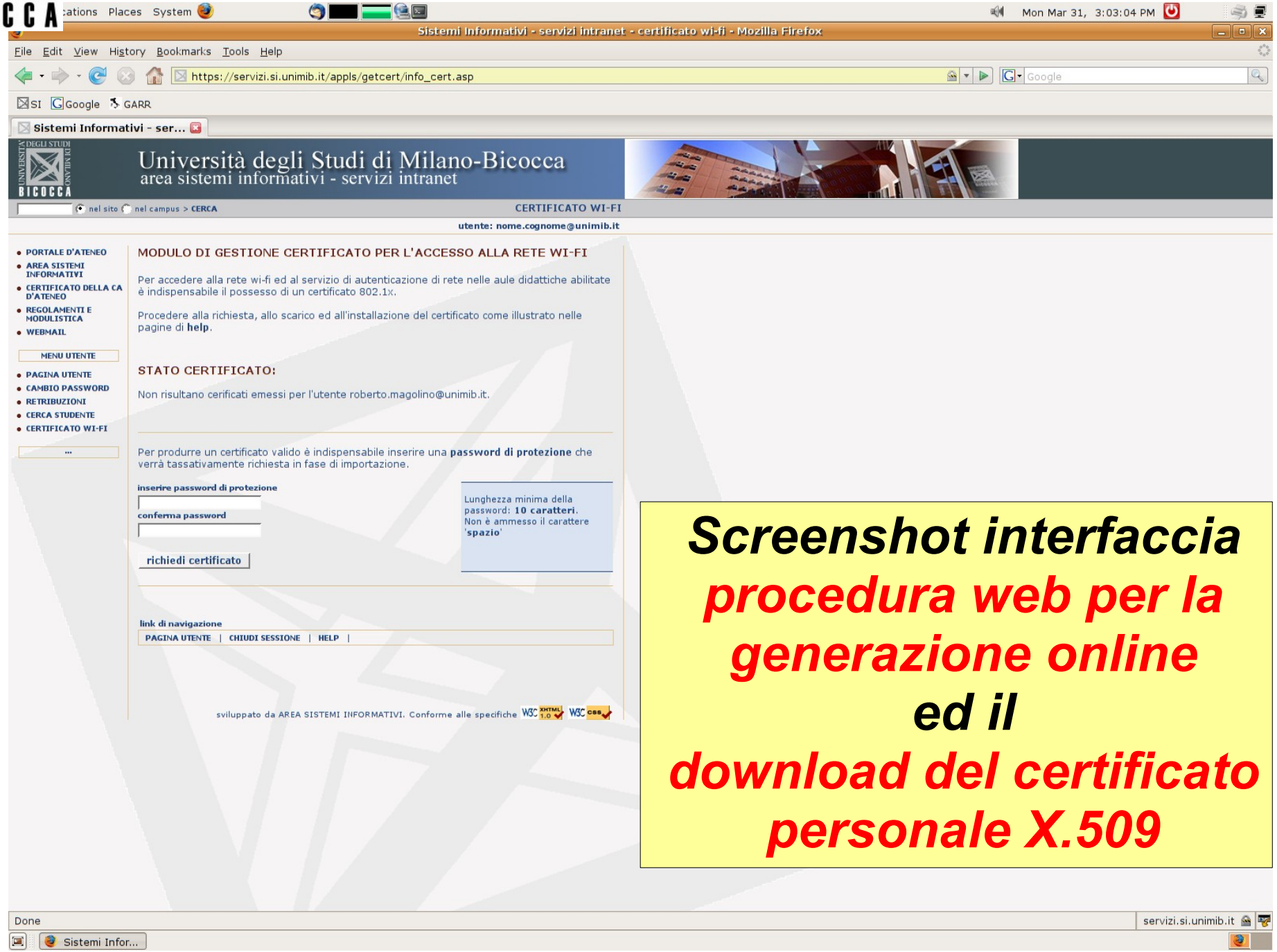
Generazione e distribuzione certificati

Tutti gli studenti e il personale strutturato, sono registrati automaticamente (con username e password) nel sistema centralizzato di autenticazione d'Ateneo rispettivamente al momento dell'immatricolazione o della presa in servizio

Con tali credenziali si autenticano, su protocollo https, al web server per la generazione online e il download del certificato personale X.509

Per I collaboratori occasionali è prevista la generazione, con le stesse modalità online, di certificati X.509 a durata limitata, su richiesta di utenti autorizzati.

Inerfaccia web per gli utenti



Screenshot interfaccia
procedura web per la generazione online
ed il
download del certificato personale X.509

Convegni e ospiti occasionali

Per la gestione dei convegni e per gli ospiti occasionali si è deciso di affiancare a 802.11i una gestione degli accessi tramite Captive Portal

I motivi che hanno portato a questa decisione si basano sulla considerazione che, a fronte di una bassa sicurezza, il servizio offerto deve essere soprattutto semplice e immediato. Le credenziali generate, username e password di durata limitata e non utilizzate per altri scopi, non hanno la criticità delle credenziali degli utenti strutturati

Per la generazione di tali credenziali si è realizzata una interfaccia web riservata all'organizzazione del convegno e al personale preposto alla gestione degli ospiti

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Reti wireless pubblicate

Accesso e inserimento nella VLAN in funzione del SSID della rete e del REALM del supplicant:

nome.cognome@unimib.it
nome.cognome@campus.unimib.it
nome.cognome@ospiti.unimib.it

I REALM relativi ad istituzioni aderenti al progetto Eduroam vengono "proxati" al radius radius.garr.net

SSID Eduroam
Rete ad accesso autenticato "proxato" a radius.it con accesso ai servizi di Ateneo e con accesso internet

SSID Unimib-conf
Rete privata a libero accesso su Captive Portal per informazioni e istruzioni per l'accesso alle reti sotto autenticazione

SSID Unimib-guest
Rete ad accesso autenticato tramite Captive Portal con accesso internet

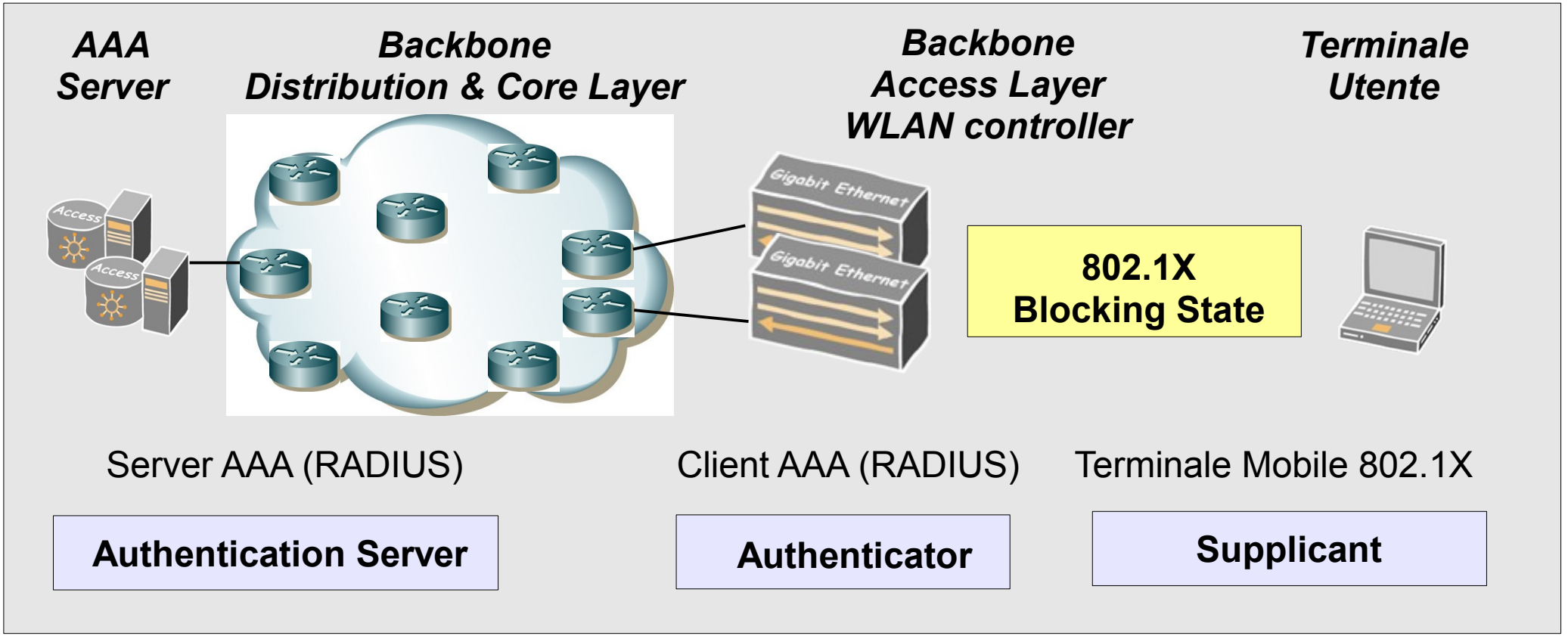
SSID Unimib-Labx
Rete privata accesso autenticato EAP-TLS con certificato X.509 con accesso ai servizi del determinato laboratorio

SSID Unimib
Rete ad accesso autenticato EAP-TLS con certificato X.509 con accesso ai servizi di Ateneo e con accesso internet

Accesso wireless (1)

L'utente accende il terminale

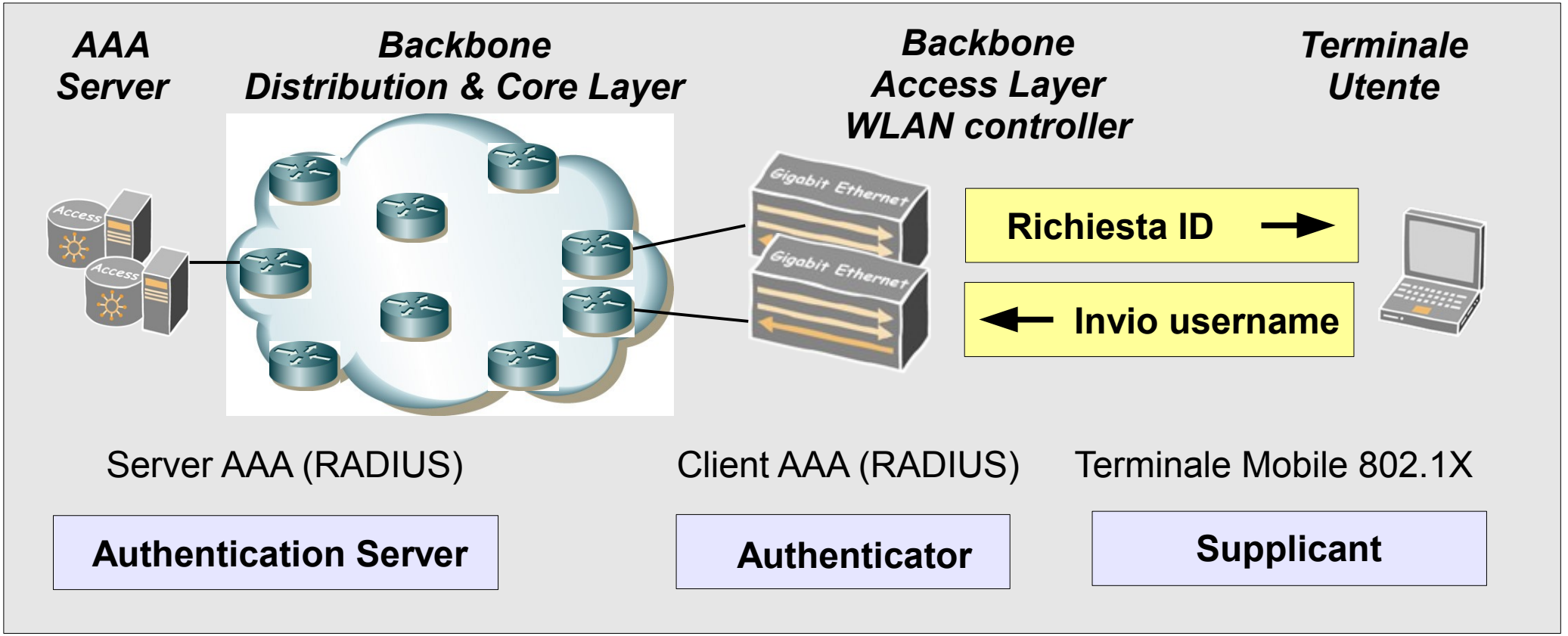
Il client X-supplicant si connette all'apparato di rete (Authenticator)



SSID reti wireless EAP-TLS: unimib, unimib-labX

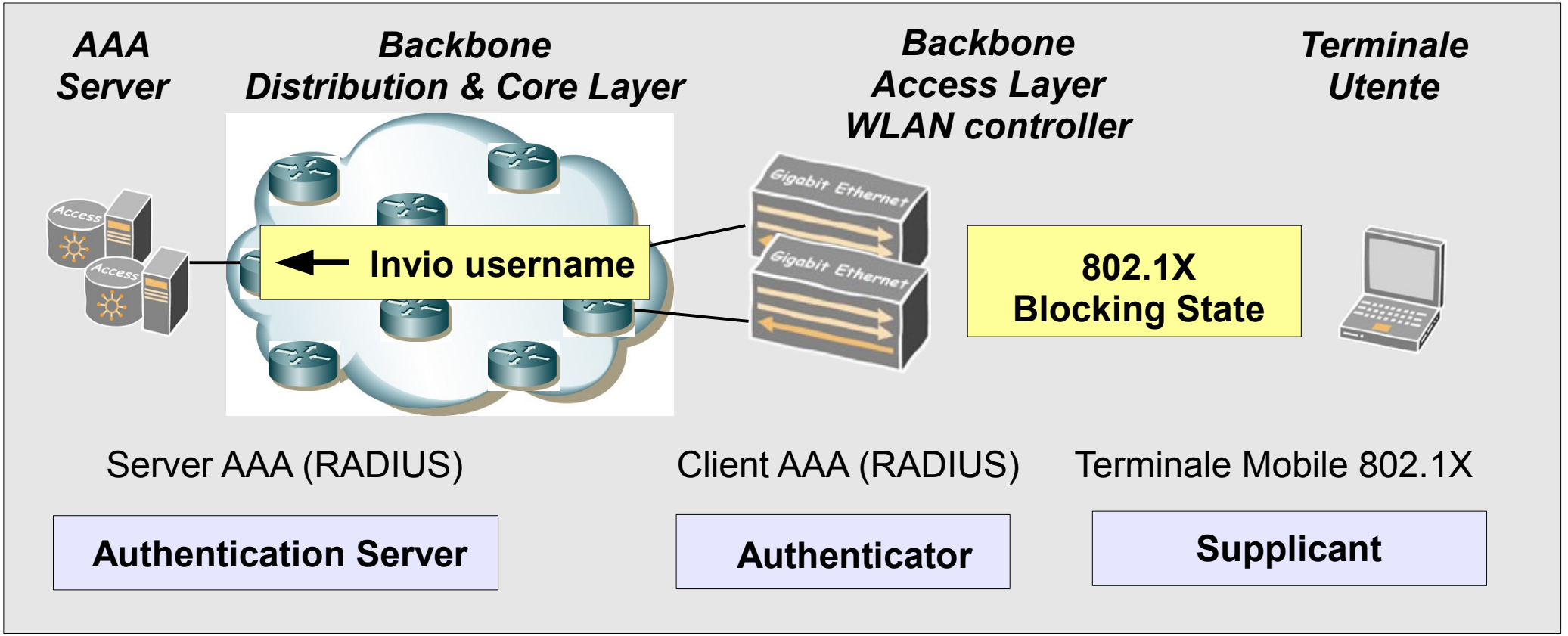
Accesso wireless (2)

Inizia il processo di autenticazione con la richiesta username



Accesso wireless (3)

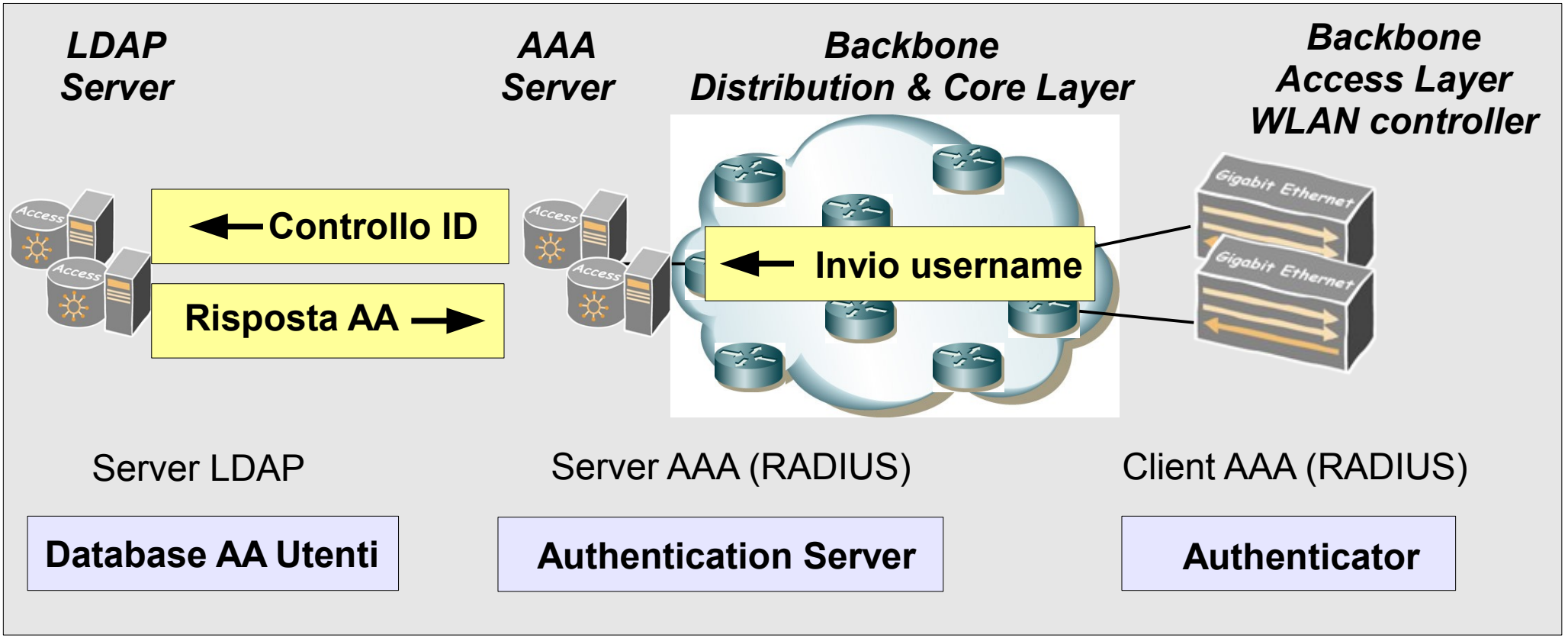
L'Authenticator riceve la richiesta di accesso del supplicant e la inoltra con lo username al server RADIUS



Accesso wireless (4)

Il server RADIUS si interfaccia con il database degli utenti

Verifica LDAP di username e dell'autorizzazione

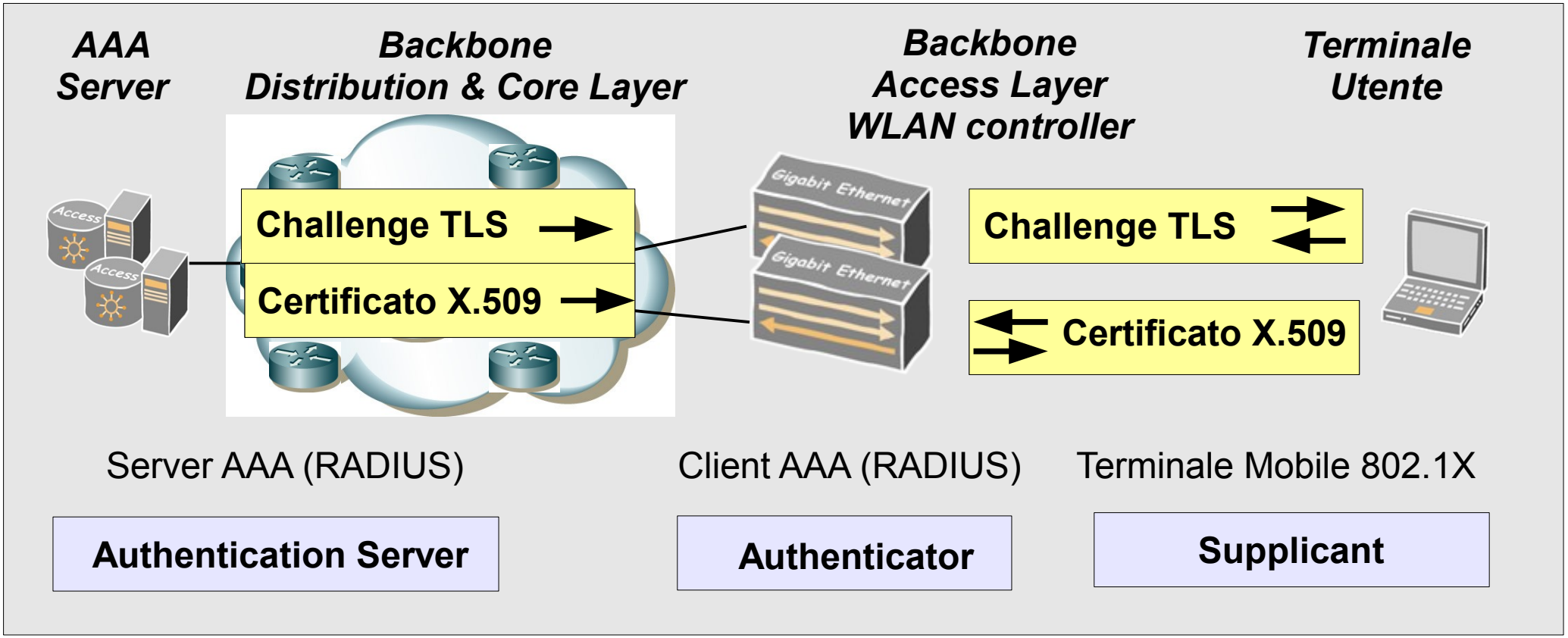


Accesso wireless (5)

RADIUS invia la "challenge" TLS e avviene lo scambio dei certificati X.509 con il mutuo riconoscimento tra client e server

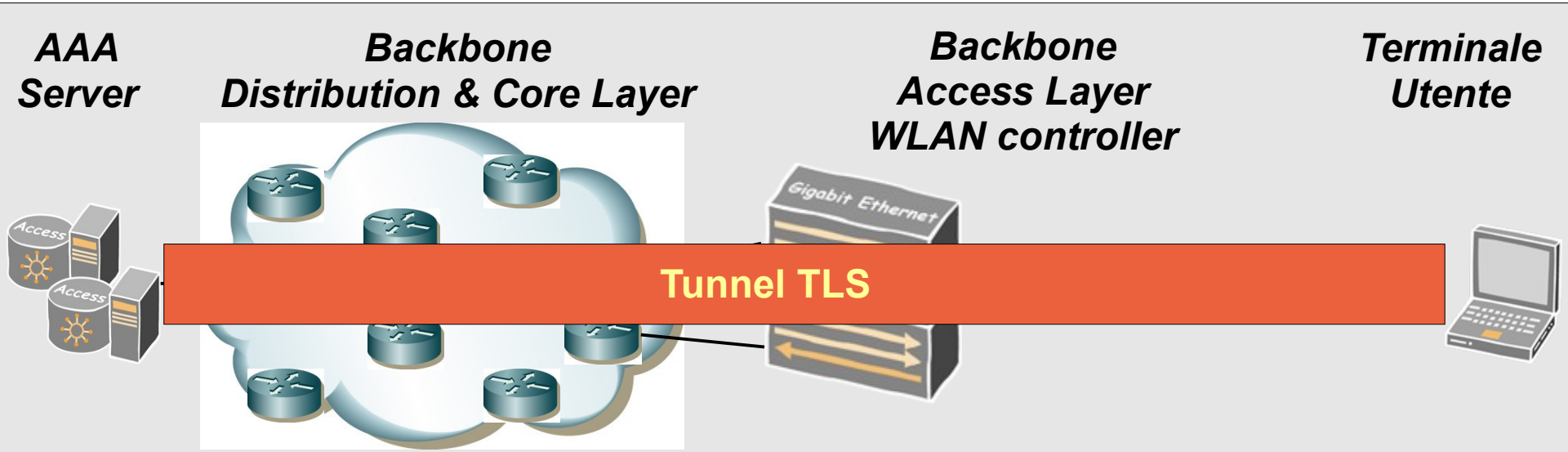
EAP-TLS: tutto avviene trasparentemente all'utente

EAP-TTLS: in questa fase l'utente immette la password



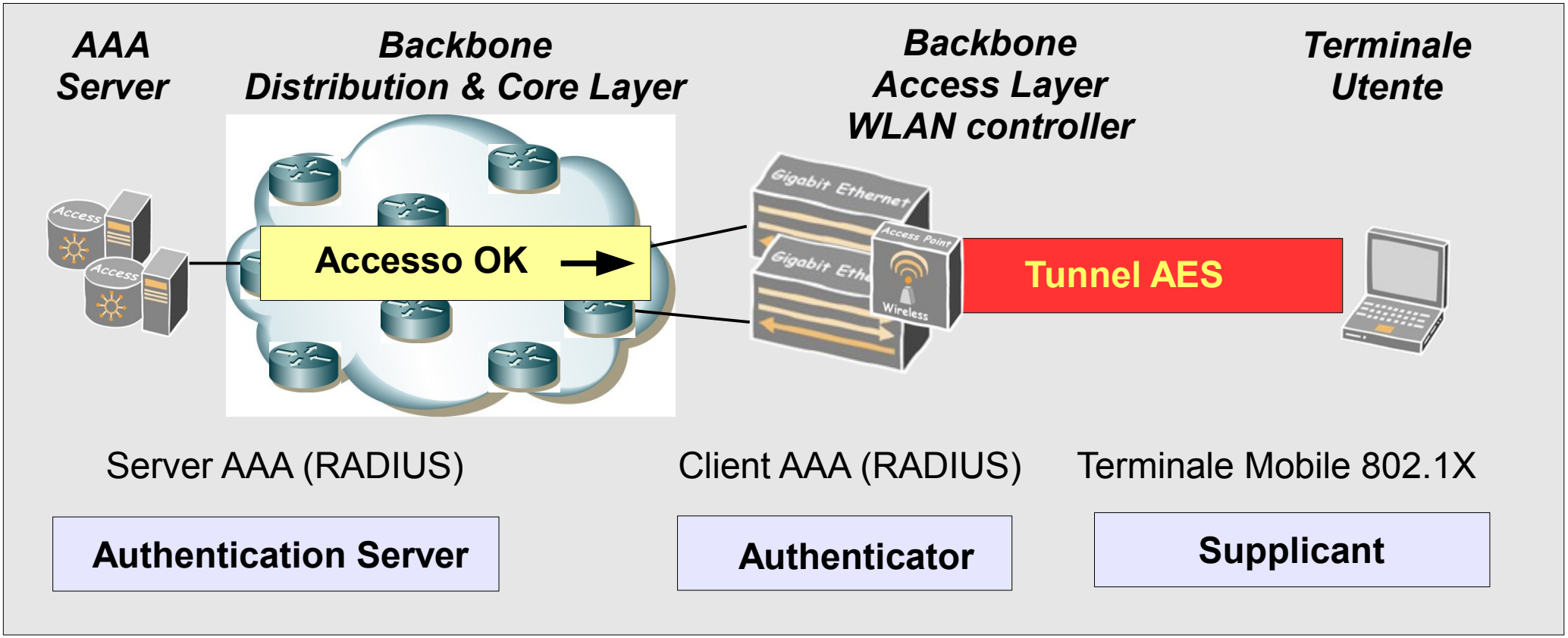
Accesso wireless (6)

Instaurato il tunnel TLS avviene la negoziazione del materiale crittografico per la cifratura del canale wireless



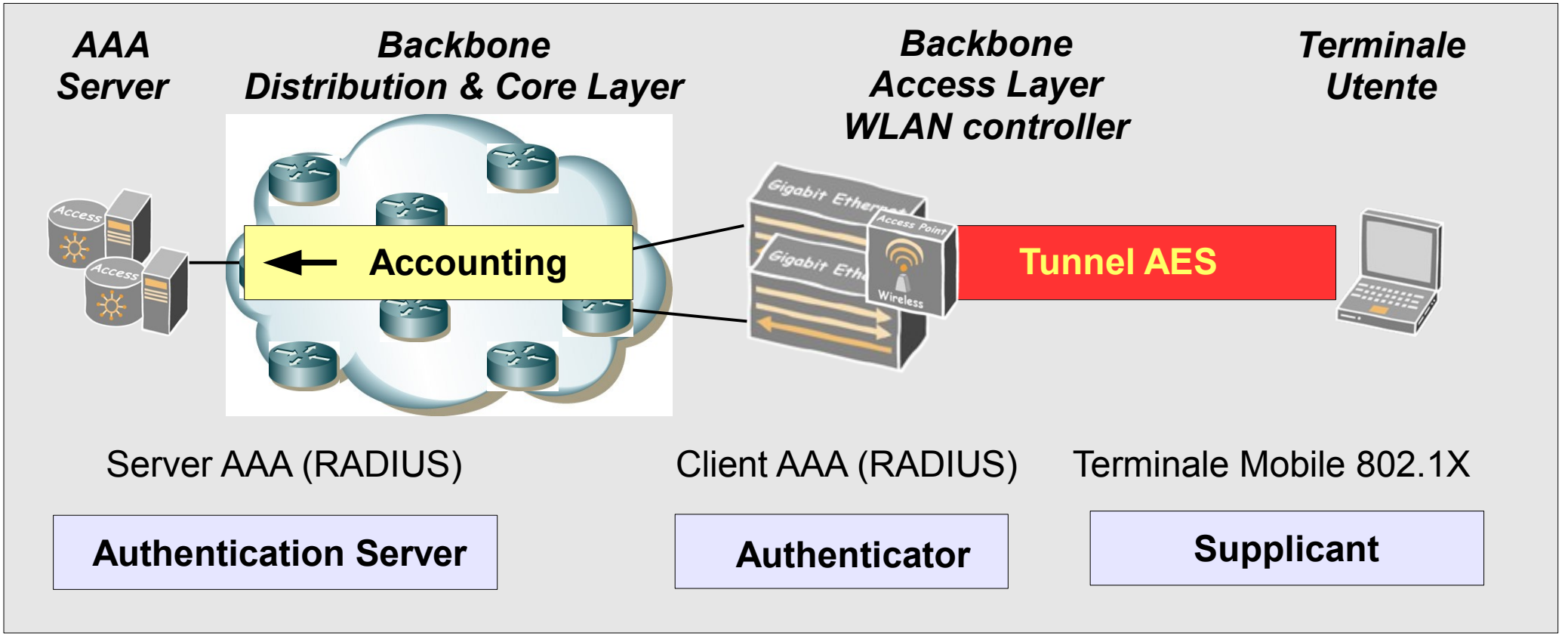
Accesso wireless (7)

Si chiude la fase di Autenticazione e Autorizzazione.
L'Autenticator riceve la PMK dal server radius, la passa all'AP,
configura la porta di accesso nella VLAN corretta
e la mette in stato di "forwarding" per il traffico utente



Accesso wireless (8)

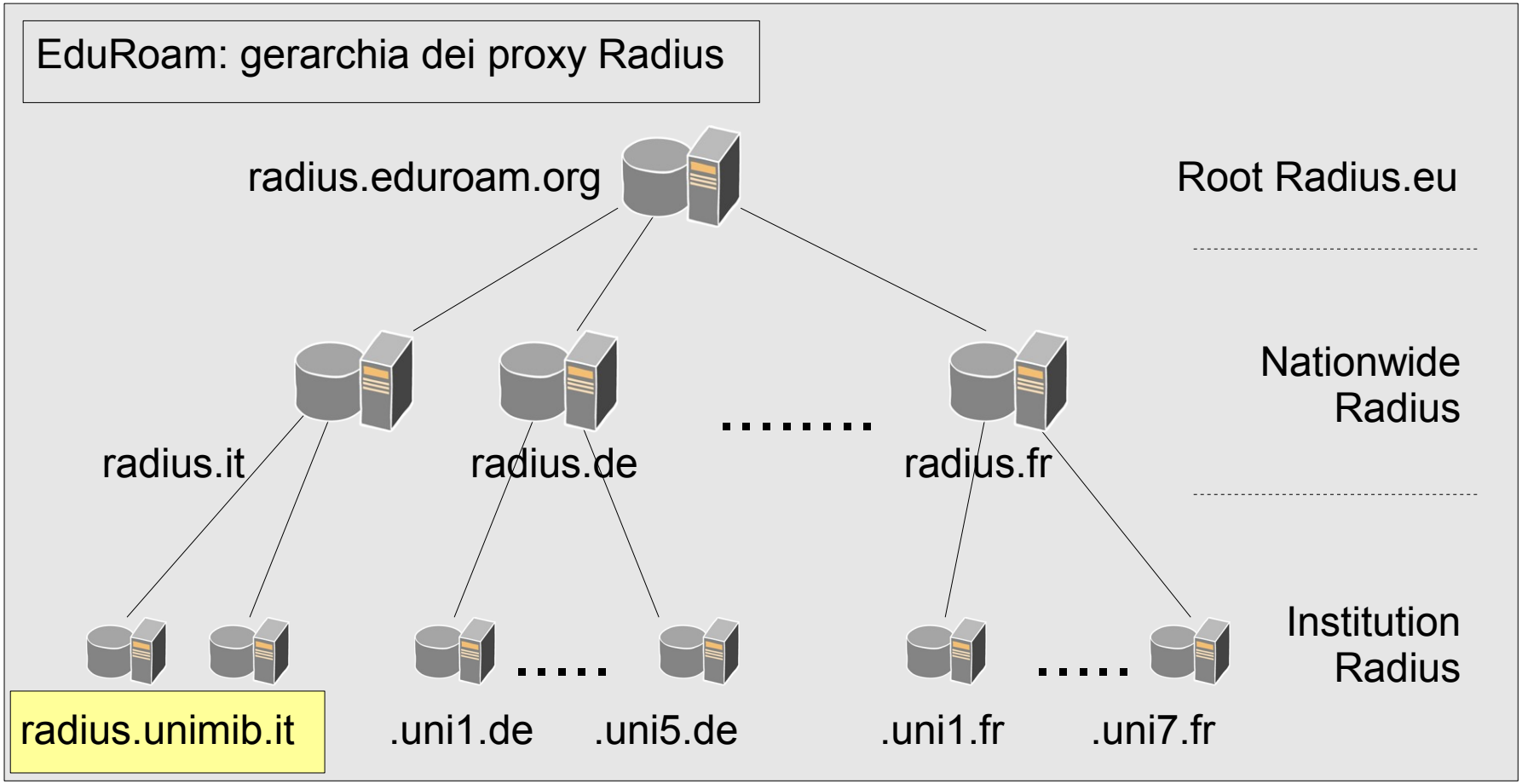
Il supplicant riceve tramite DHCP l'indirzzo IP ed entra in rete.
L'Authenticator inizia la fase di Accounting con il server RADIUS



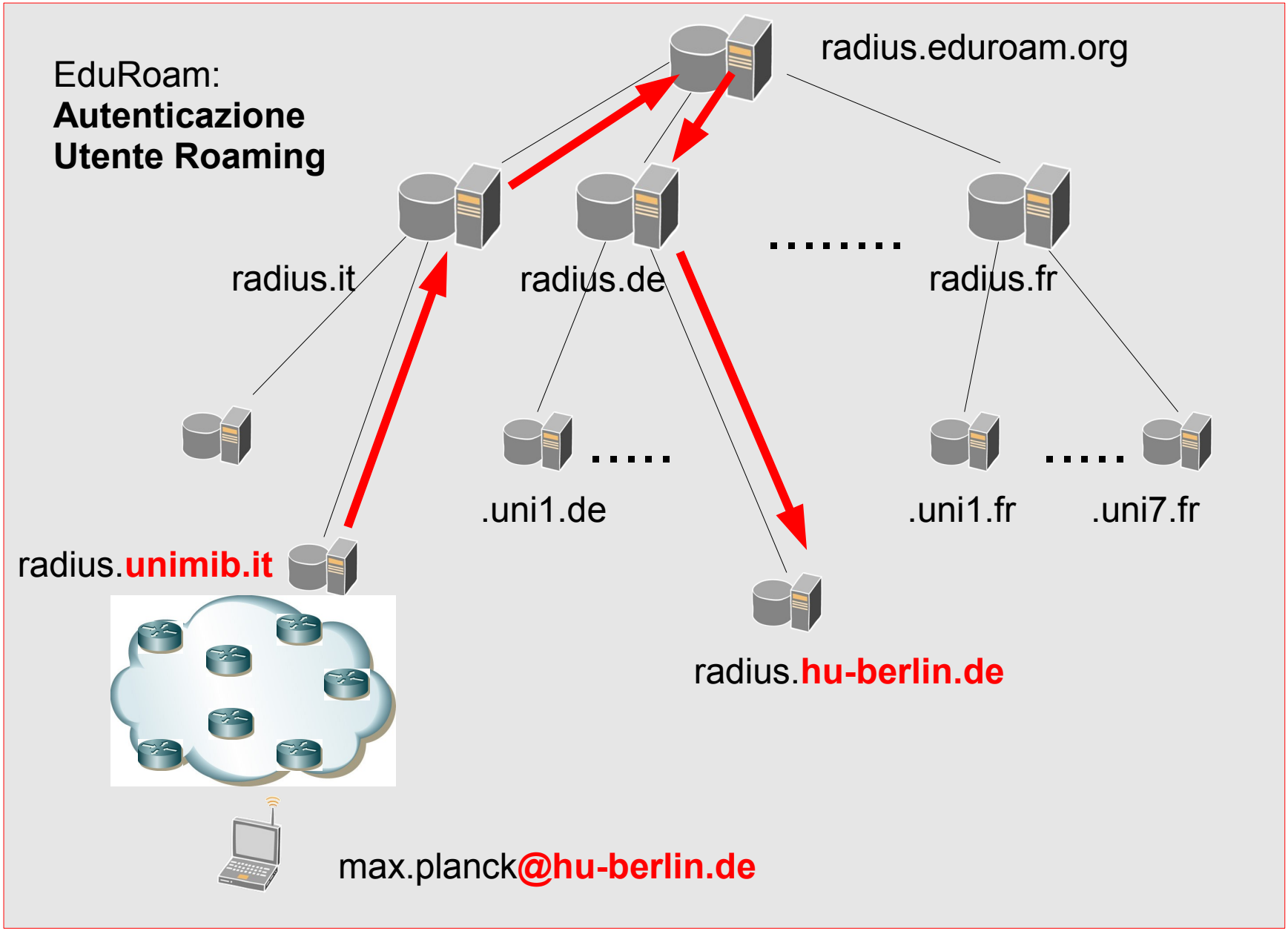
Accesso Eduroam

Progetto Education Roaming per la mobilità di personale e studenti

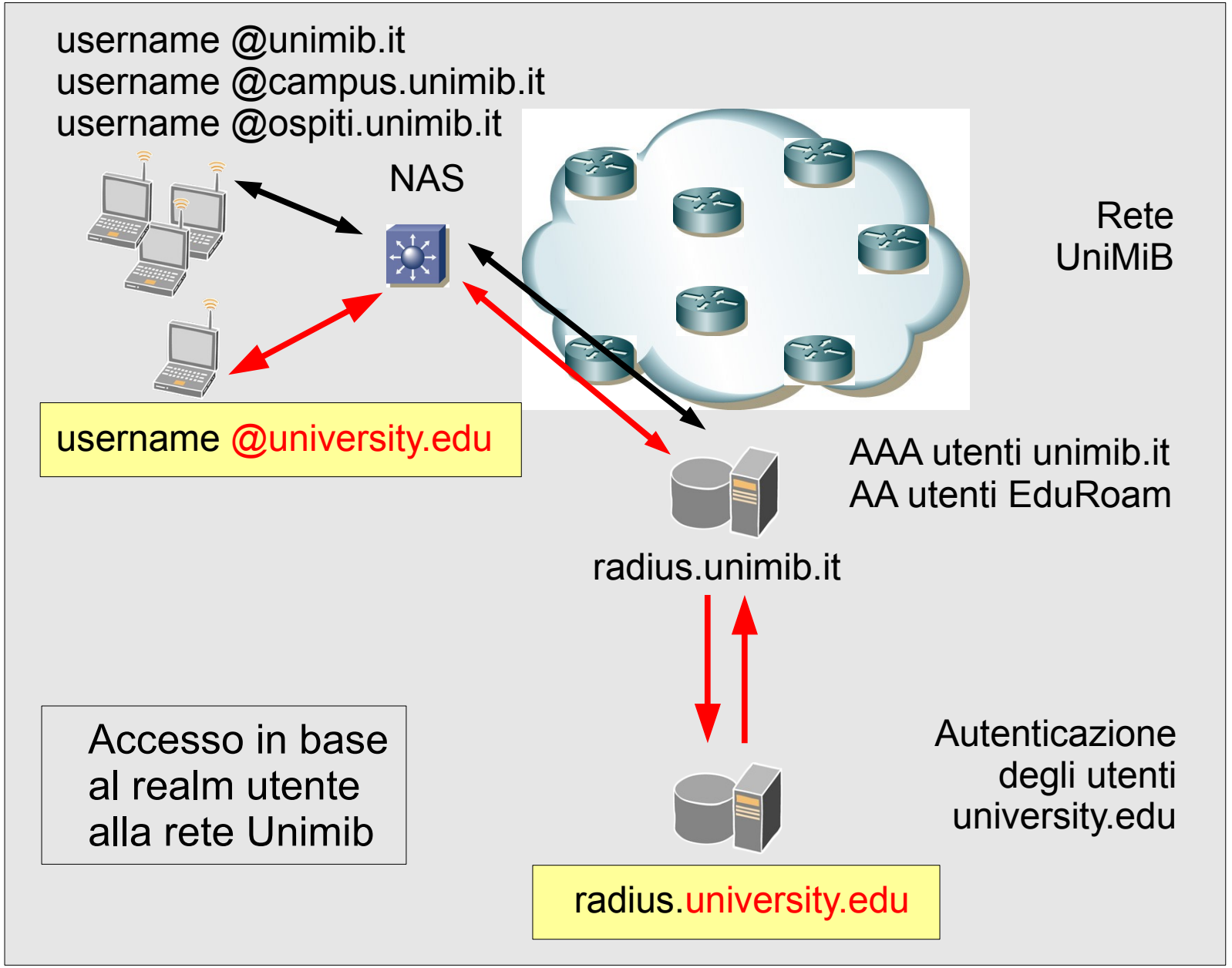
Federazione per l'autenticazione tra Università ed Enti di Ricerca



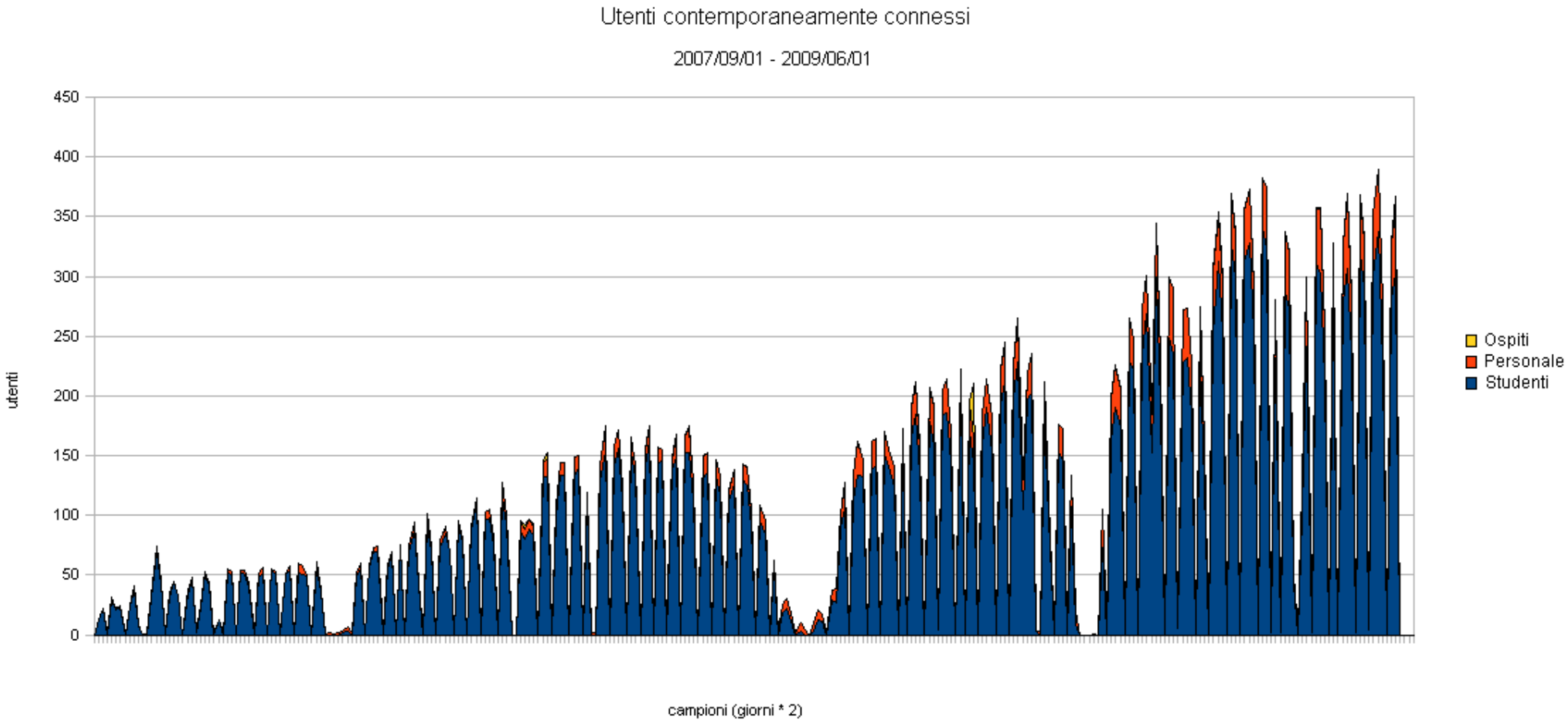
Accesso EduRoam



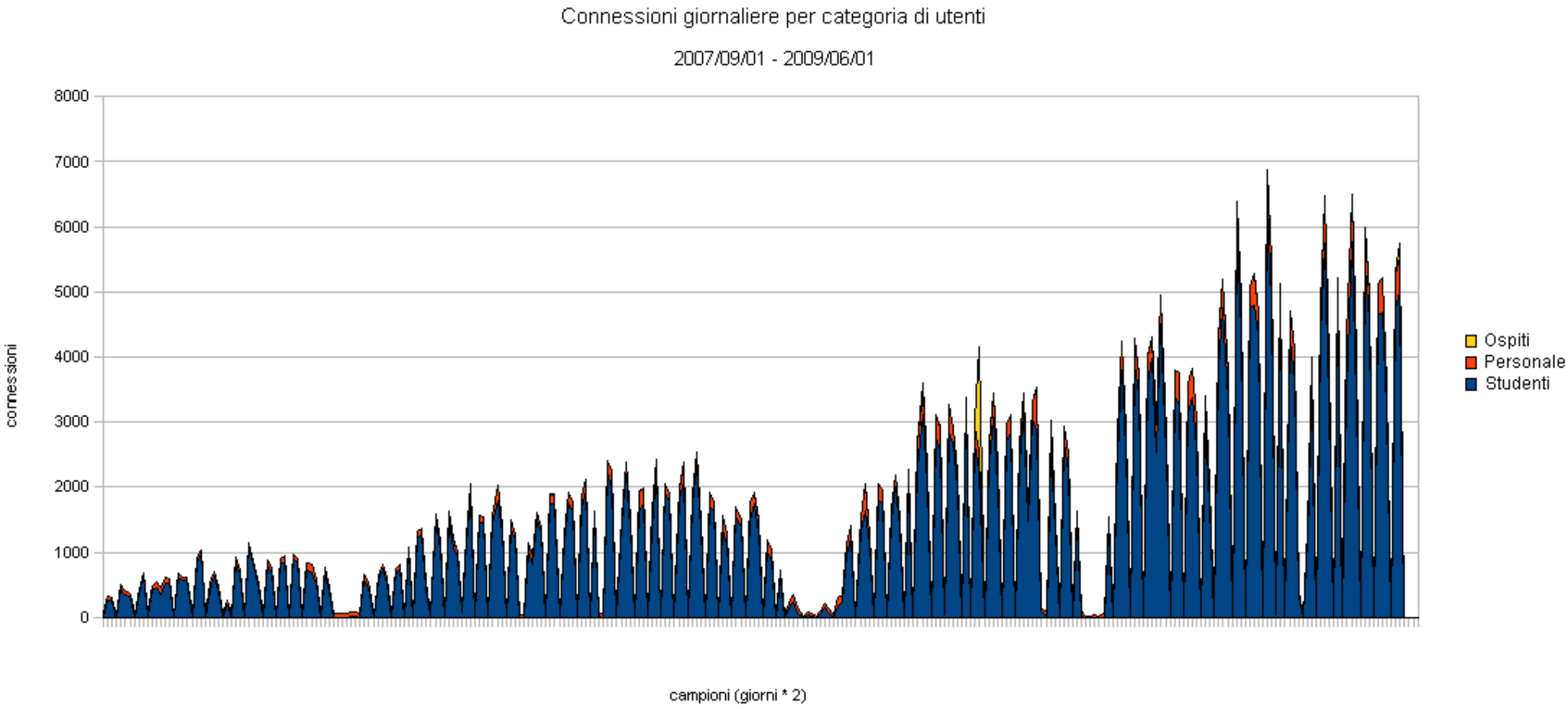
Accesso utenti Unimib e roaming Eduroam



Statistiche accessi wireless



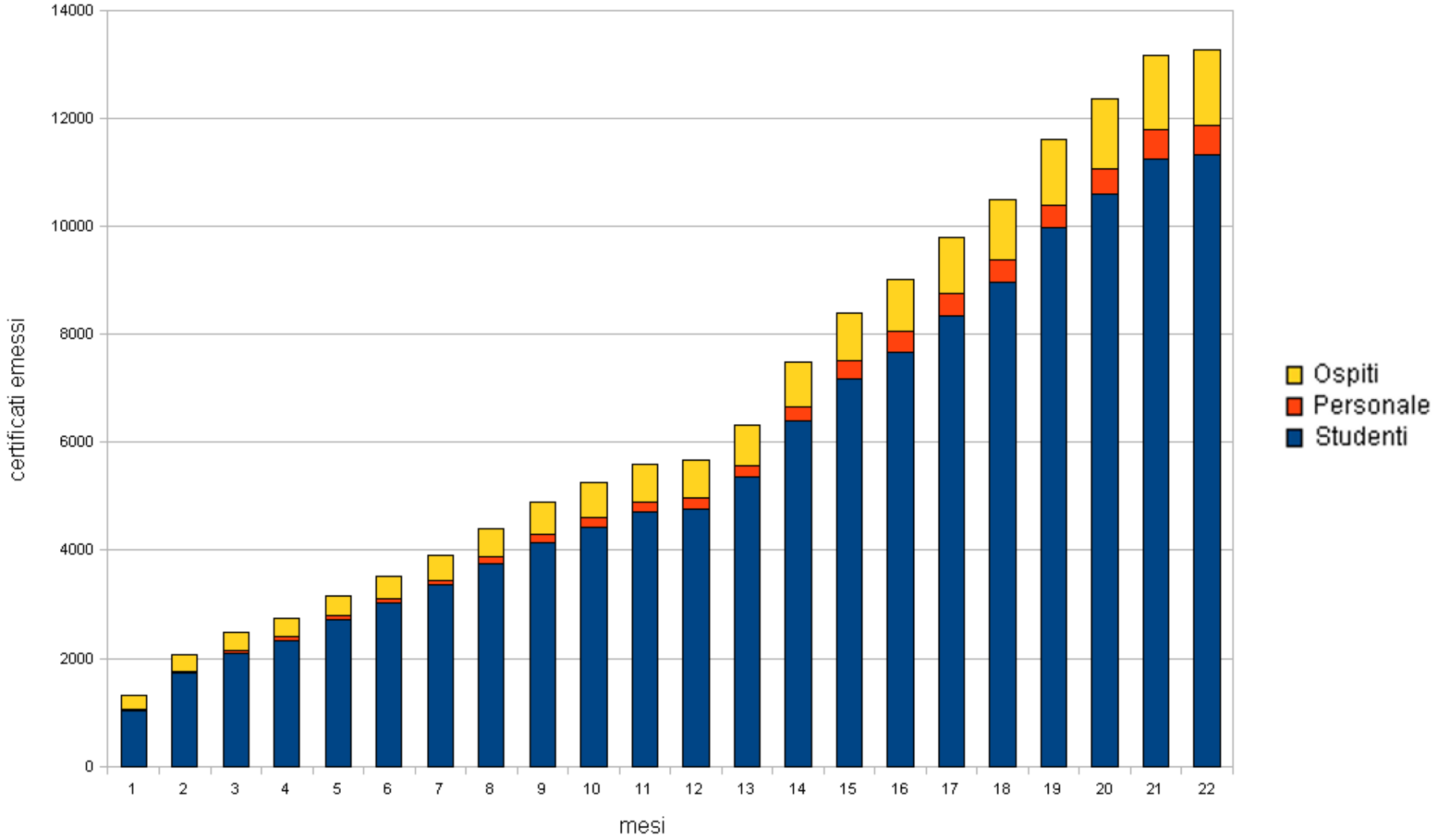
Statistiche accessi wireless



Statistiche accessi wireless

Certificati emessi, suddivisi per utenza

grafico dal 2007/09 al 2009/06 incluso



UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Requisiti

Dimensioni della base utenti e scelta del sistema di AAA (Autorizzazione, Autenticazione, Accounting)

- 40mila utenti

- 300-350 supplicant contemporaneamente connessi nella fascia oraria 08:00-17:00, in crescita costante.

- 90% studenti
- 9% personale strutturato
- 1% ospiti

- Il sistema AAA integra WiFi di Ateneo, servizo Eduroam e servizio 802.1X wired

Scelta del metodo di autenticazione

Convegni e problemi logistici correlati

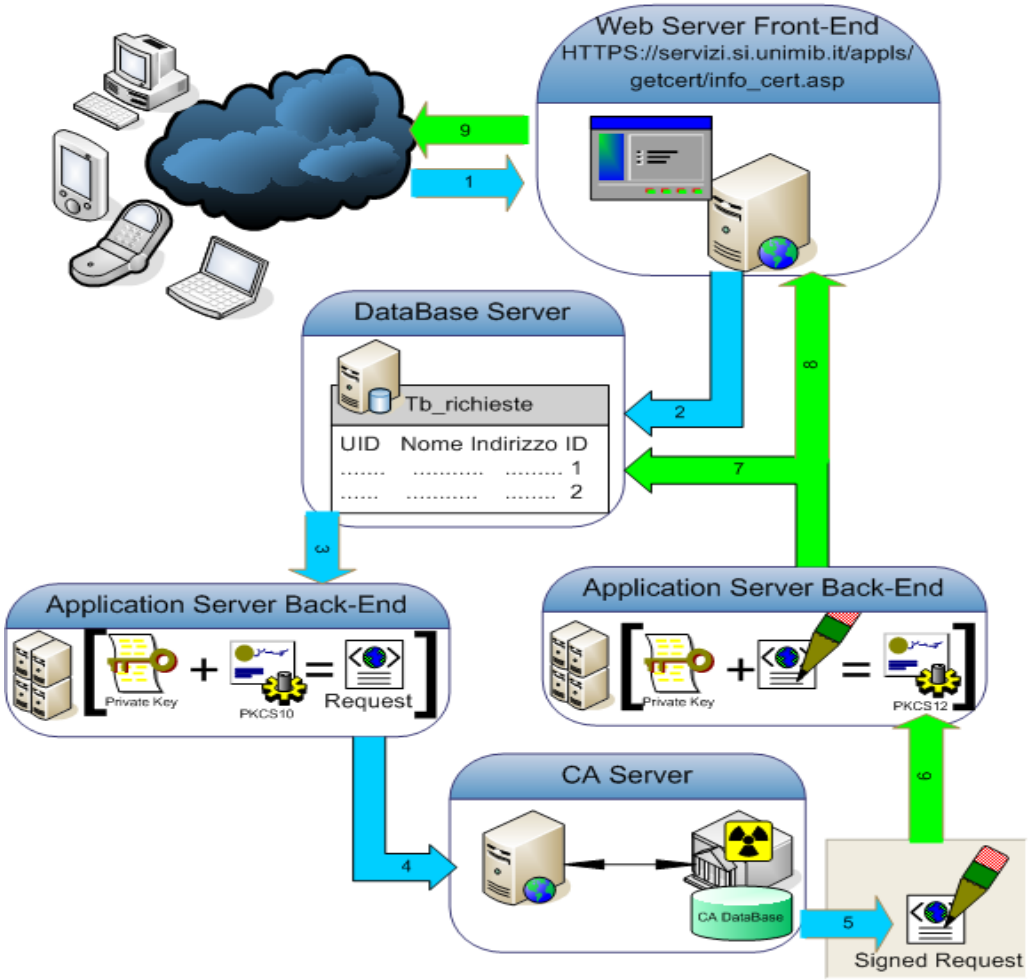
- SSL captive portal con username e password autenticati su server Radius

- SSID unimib-guest utilizzato esclusivamente per i convegni

- Il portale SSL e' integrato nel firmware dei Wlan Access Servers, l'autorizzazione e l'autenticazione vengono effettuate contro i server radius e LDAP

Gestione delle credenziali per il metodo EAP-TLS

Flusso per la generazione dei certificati d' Ateneo



1. La richiesta per la generazione di un nuvo certificato, viene inviata via web, al sito dei Sistemi Informativi.

2. La richiesta viene registrata su un DataBase Server.

3. L' Application Server si occuperà di processare ogni richiesta valida. Per ogni richiesta di nuovo certificato, viene creata una chiave privata ed un pkcs10.

4. L' Application Server, incapsula il pkcs10 in una WebRequest diretta al server di Front-End della CA.

5. Il server della CA, riceve il pkcs10 e lo "firma" con le apposite chiavi.

6. Il server della CA invia all' Application Server, il pkcs10 "firmato".

7. L' Application Server, ricevuto il pkcs10 "firmato", genera a questo punto, il pkcs12.

8. L'Application Server registra poi sul DataBase Server, in corrispondenza del profilo dell'utente che ne ha fatto richiesta, il relativo pkcs12.

9. Il pkcs12 viene presentato per il download nella pagina personale dell'utente.

Gestione delle credenziali per il metodo EAP-TLS

MODULO DI GESTIONE CERTIFICATO PER L'ACCESSO ALLA RETE WI-FI

Per accedere alla rete wi-fi ed al servizio di autenticazione di rete nelle aule didattiche abilitate è indispensabile il possesso di un certificato X.509.

Procedere alla richiesta, allo scarico ed all'installazione del certificato come illustrato nelle pagine di **help**.

STATO CERTIFICATO:

serial n.	**018EC7**
richiesto	**01/07/2008**
emesso	**01/07/2008**
validità	**01/07/2008 - 01/07/2009**
download	**01/07/2008**
richiesta revoca	
revoca	

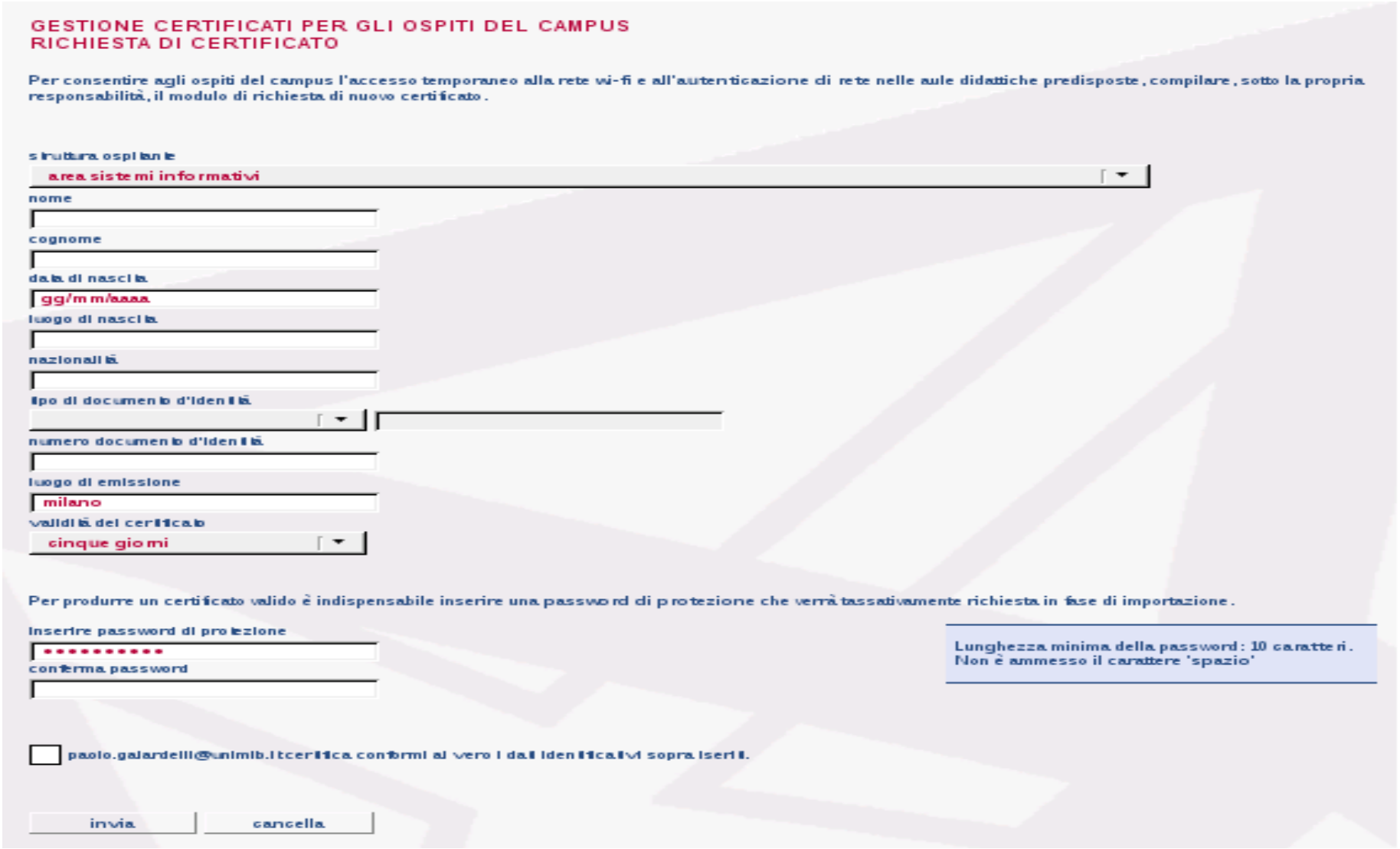
Il certificato in suo possesso è **valido**.

revoca certificato

link di navigazione

PAGINA UTENTE | CHIUDI SESSIONE | HELP |

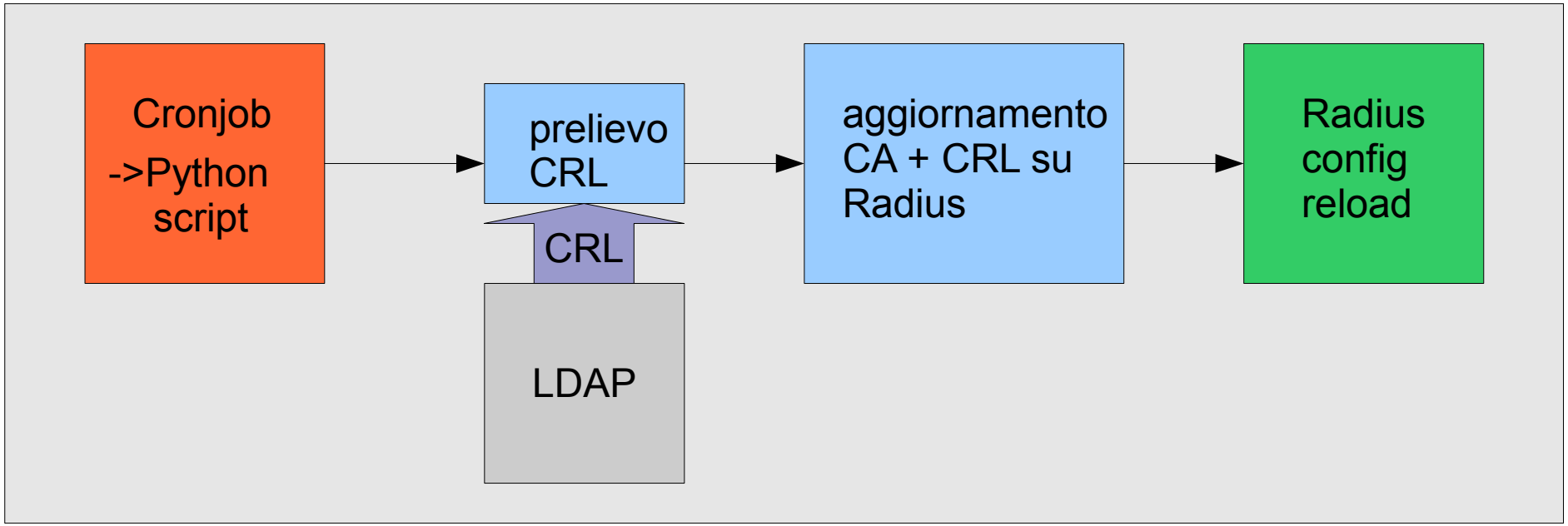
Gestione delle credenziali per il metodo EAP-TLS



Implementare il metodo di autorizzazione e autenticazione

Certificati e FreeRadius

- Richiesti gli *utilizzi estesi* ***TLS*** **server authentication** e **TLS client authentication**
- Eseguito il controllo User-Name == CN del certificato fase AA
- La CRL viene gestita e aggiornata via cronjob e script in python

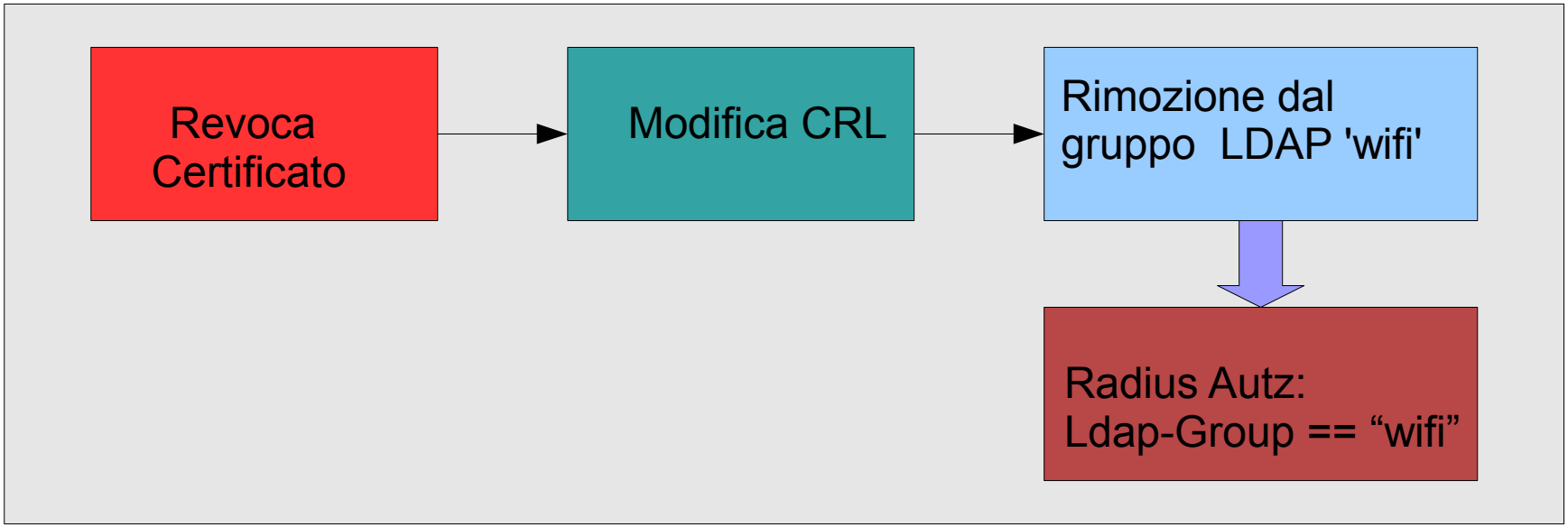


Imprevisti nella gestione dei certificati: impatto relativo alla fase di autorizzazione

Il periodo di validita' di ogni certificato emesso e' pari ad un anno, tuttavia:

- L'utente ha revocato il proprio certificato ma la CRL non e' ancora stata aggiornata sul server Radius (aggiornamenti ogni ora)

- L'utente ha cessato i rapporti con l'ateneo ma il certificato e' ancora valido



Implementare la gestione dei Realm in fase di autorizzazione

```
# estratto dal file /etc/raddbproxy.conf

realm DEFAULT {
        type            = radius
        authhost        = radius.garr.net:1812
        accthost        = LOCAL
        secret          = SECRET
        nostrip
}
```

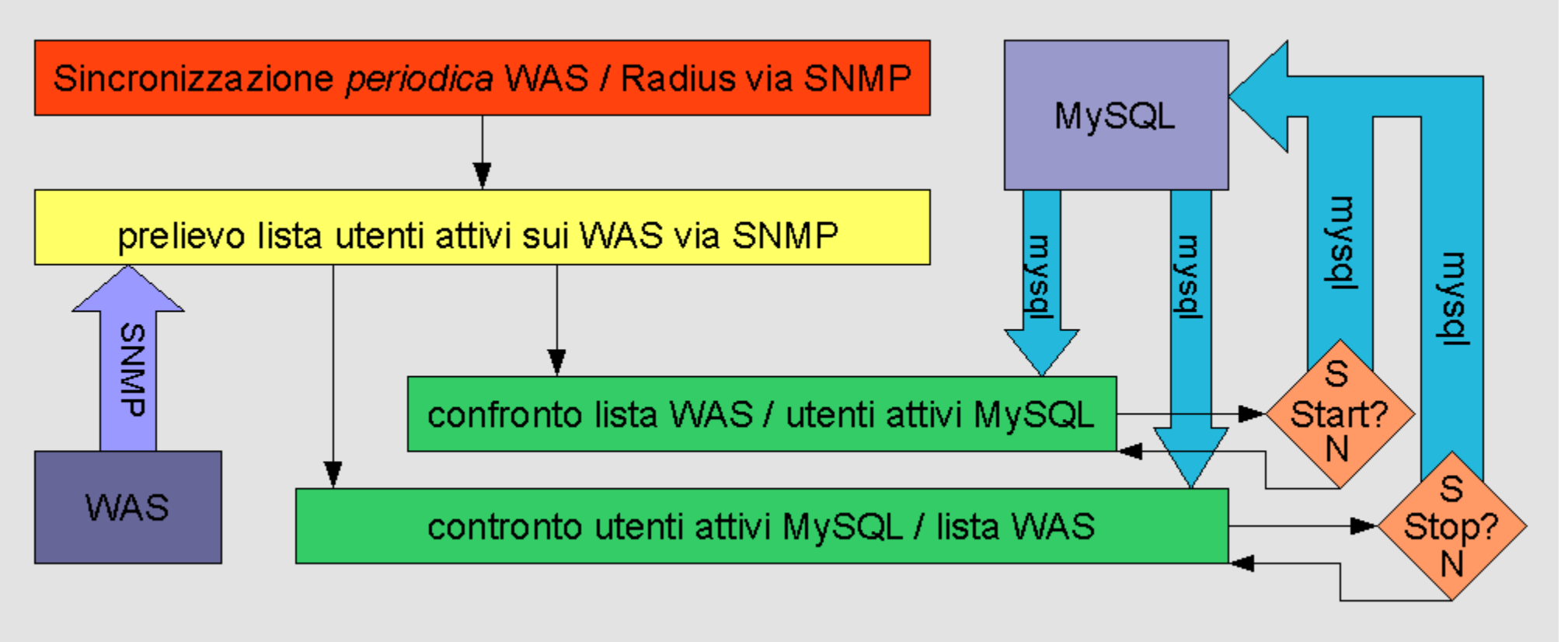
Accounting eduroam gestito localmente per garantire l'associazione nome utente - IP

```
# estratto dal file /etc/raddb/hints

DEFAULT         suffix == "ospiti.unimib.it"
       Ldap-UserDn = `uid=%{User-Name},ou=ospiti,dc=unimib,dc=it`

# questa sezione forza, per I soli ospiti la sola ricerca dell'oggetto
# nel gruppo LDAP 'wifi', ou 'ospiti'
```

Ricerca di oggetti che non esistono nell'albero utenti di LDAP

Accuratezza dell'accounting e problemi correlati

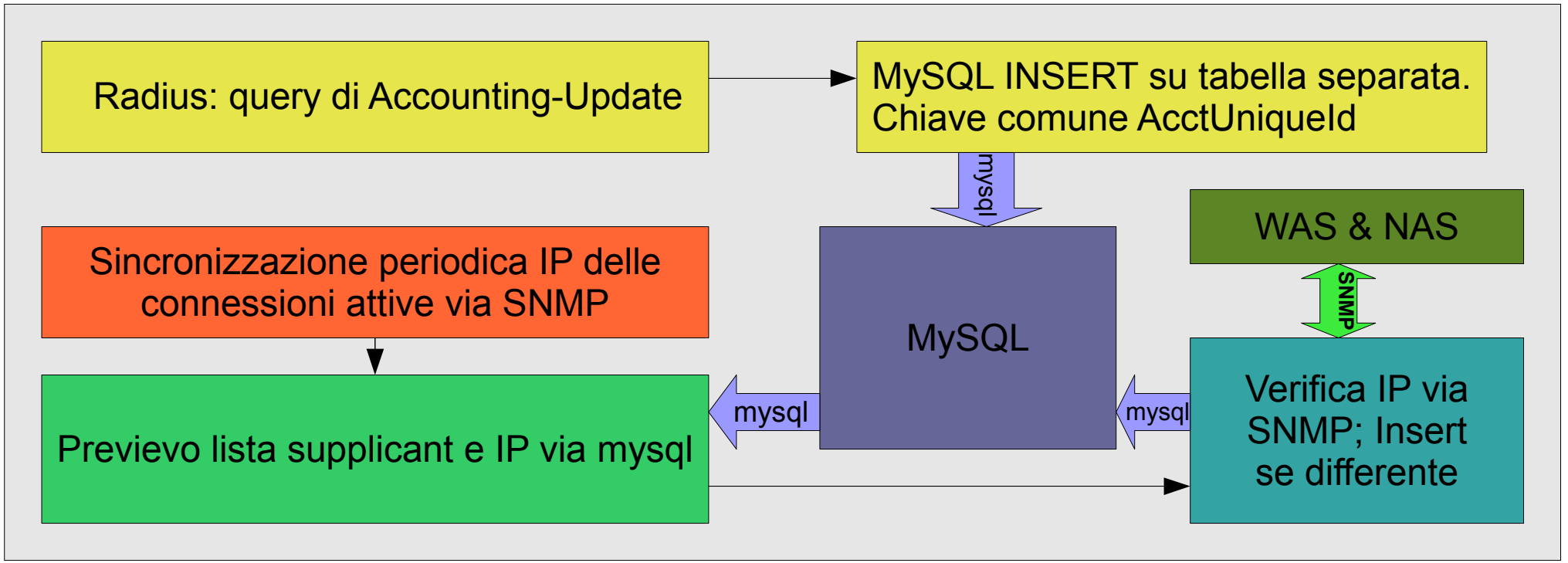
- **Ravvio hardware AP e WAS**: utenti disconnessi senza radius accounting-stop.
- **Aggiornamento della CRL con SIGHUP / SIGKILL**: impossibile preservare lo stato delle transazioni EAP incomplete.



Implementazione del sistema di Accounting

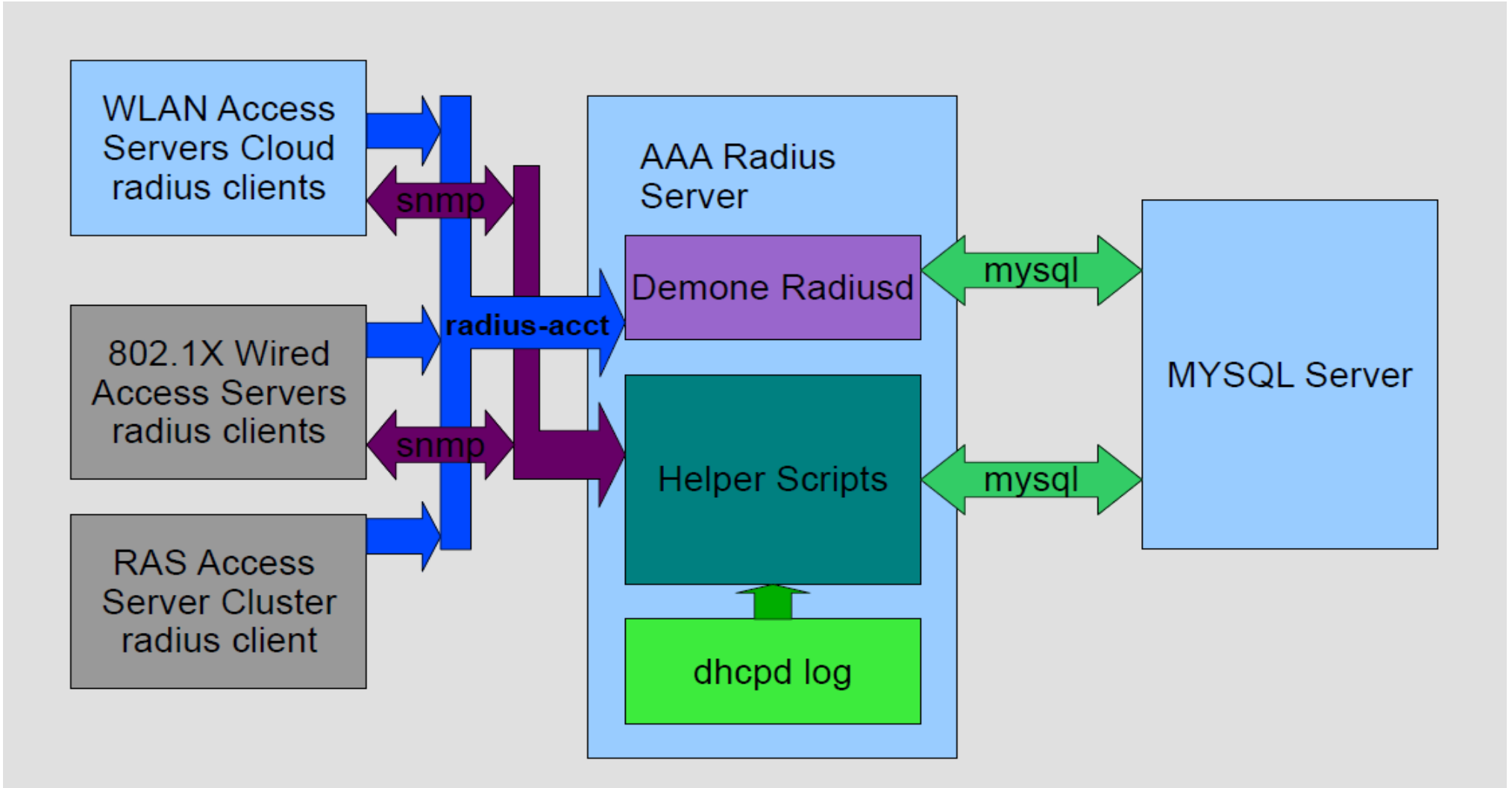
- Evasione accounting: se il WAS dovesse riconoscere un cambio di IP del supplicant generando un update, andrebbe a sovrascrivere il FramedIPAddress

- DHCP lease variabile: l'informazione relativa al FramedIPAddress verrebbe sovrascritta al cambio di IP



Implementazione del sistema di Accounting

Flussi di Accounting, schema completo



Monitoraggio e gestione del sistema

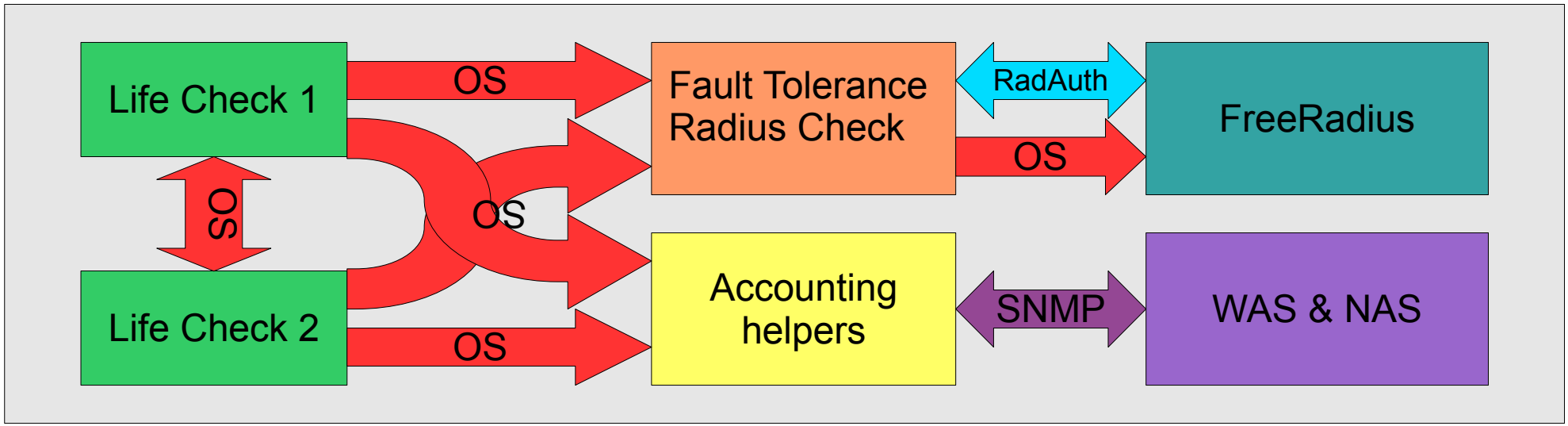
Interventi di gestione ordinaria ripetitiva del server

- via crontab i log del demone radiusd vengono periodicamente compressi e datati e ruotati
- la CRL viene aggiornata, controllo fault tolerance sospeso e riavviato

Fault tolerance

- necessita' di identificare tempestivamente eventuali malfunzionamenti del sistema

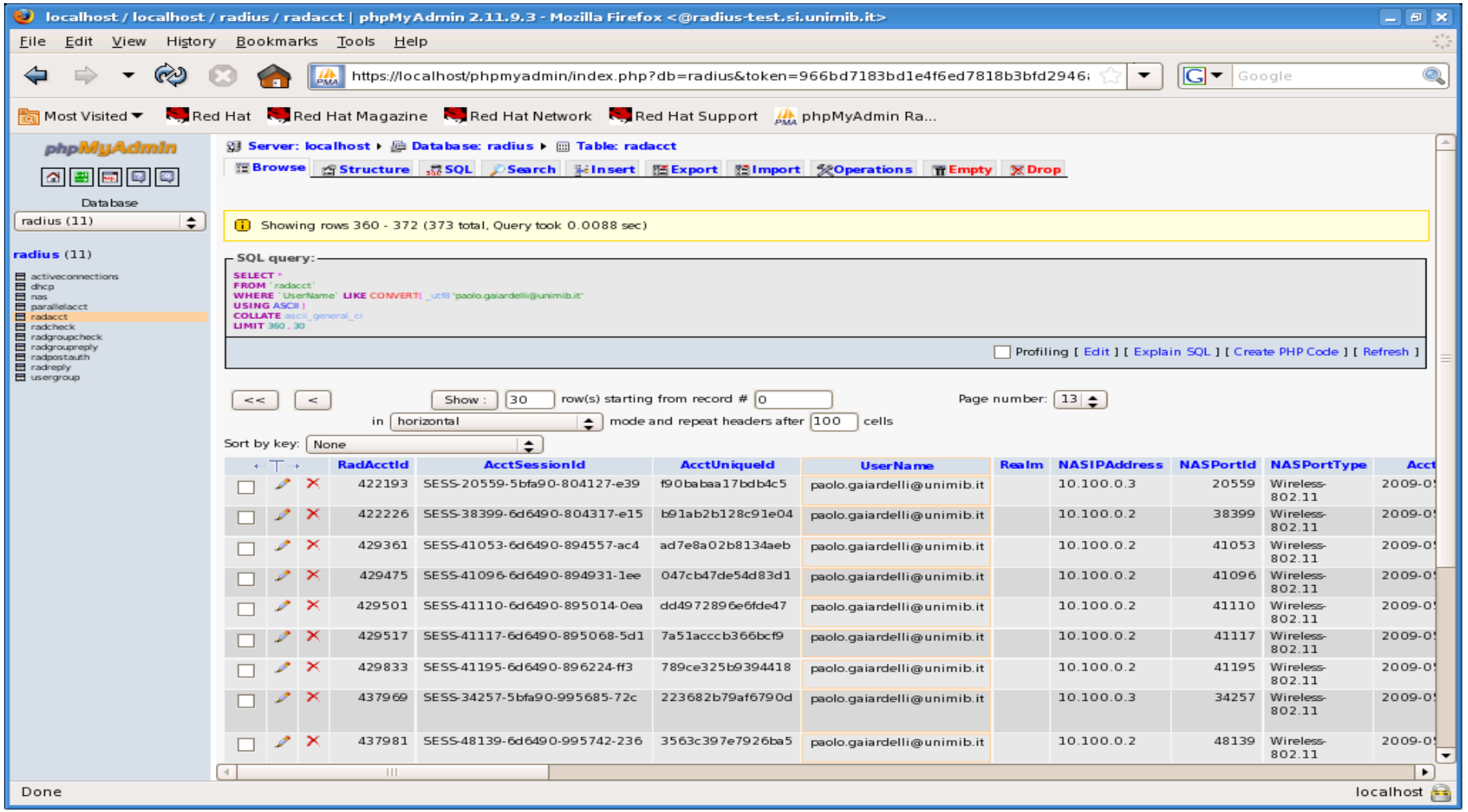
- viene eseguita periodicamente la verifica di "esistenza in vita" dei demoni e degli helper



UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Strumenti diagnostici

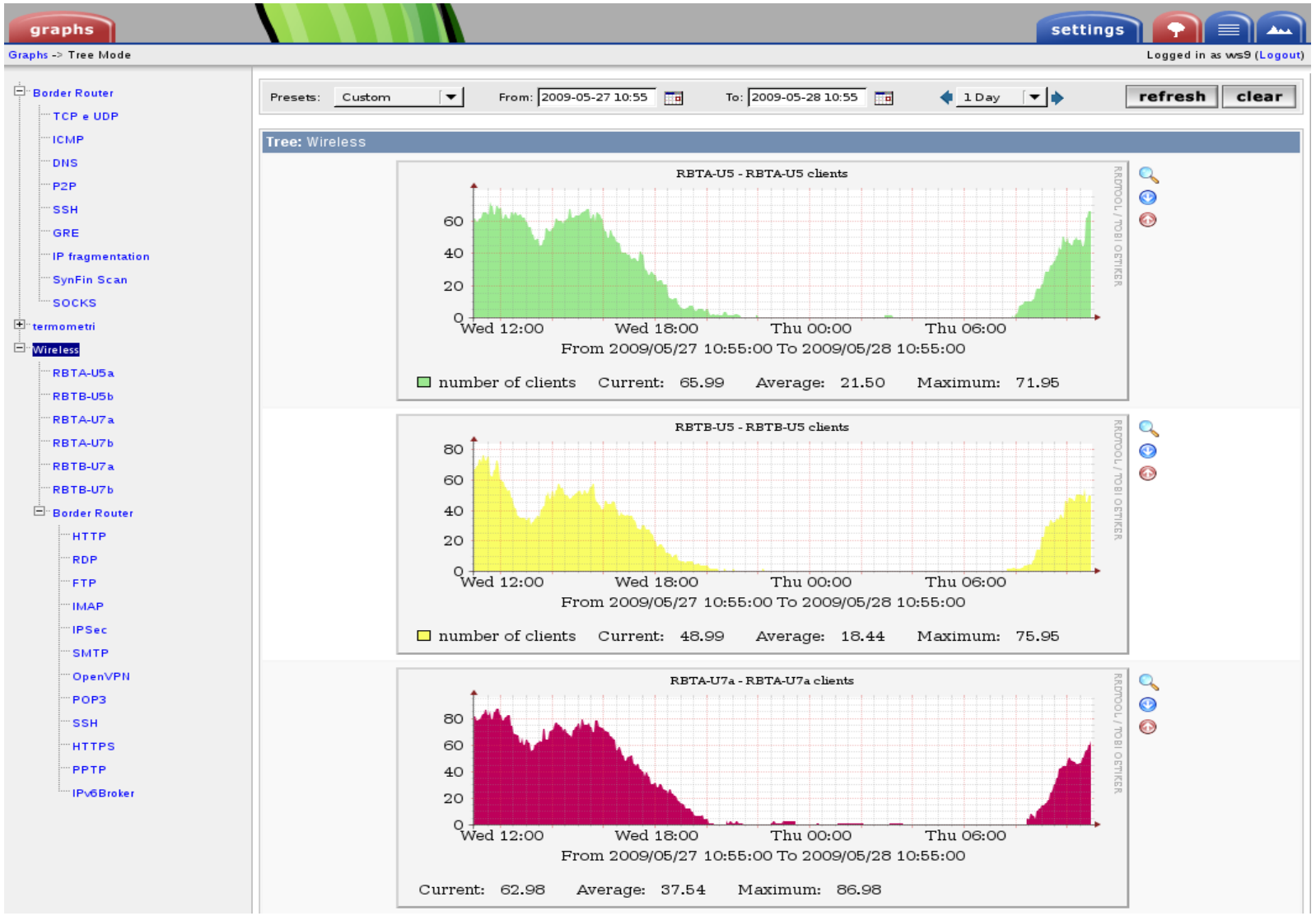
PHPMyAdmin

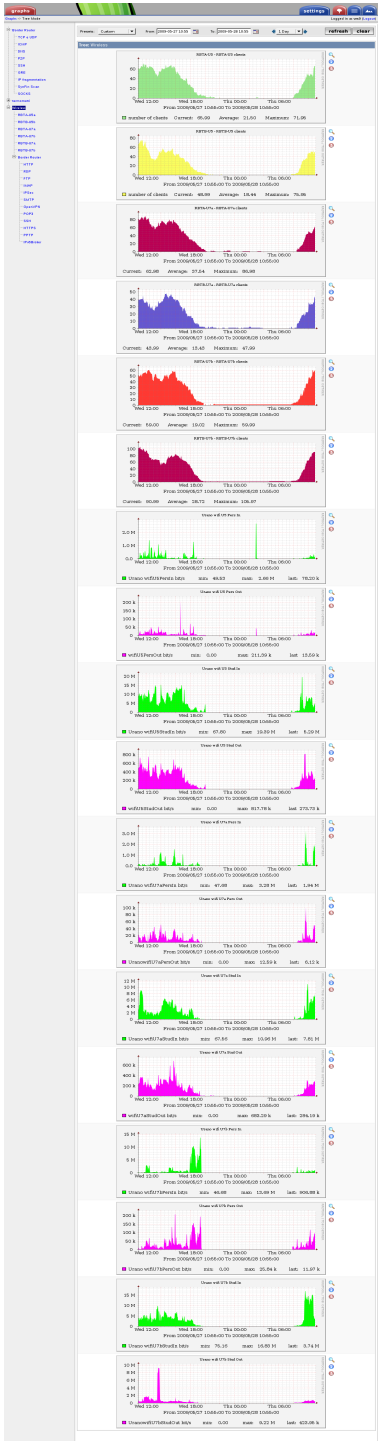


UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Strumenti diagnostici

Cacti





UNIVERSITA' DEGLI STUDI DI MILANO BICOCCA

Gestione Utenti

- *I supplicant classici (macchine Windows XP e Vista, Linux, Mac) sono stati testati*

- *I supplicant non convenzionali* (PDA, cellulari con wifi, iPod e simili, netbook e internet tablets) sono stati testati, ma *non sono ufficialmente supportati*

- *E' stato creato un help online con il livello di dettaglio piu' elevato possibile*.

Gestione Utenti

C

Hardware e Software

- *Si osserva che circa il 5% dei supplicant ha problemi*

Le cause osservate sono nell'ordine:

- *hardware di rete difettoso*, scarsa sensibilita' in ricezione, scarsa potenza in trasmissione.

- *il sistema operativo e' eccessivamente danneggiato* o compromesso

Gestione Utenti

Helpdesk

- emessi circa 13000 certificati
- 6000 certificati attivi
- richieste di assistenza registrate: 180 (+ ~40 richieste non registrate)
- una richiesta ogni 4 giorni