Realizzazione di hotspot wireless per l'Università degli Studi di Milano

Marcello Meroni, Michele de Varda,
DIVISIONE TELECOMUNICAZIONI
UNIVERSITÀ DEGLI STUDI DI MILANO
Workshop GARR-X, 3 Aprile 2008

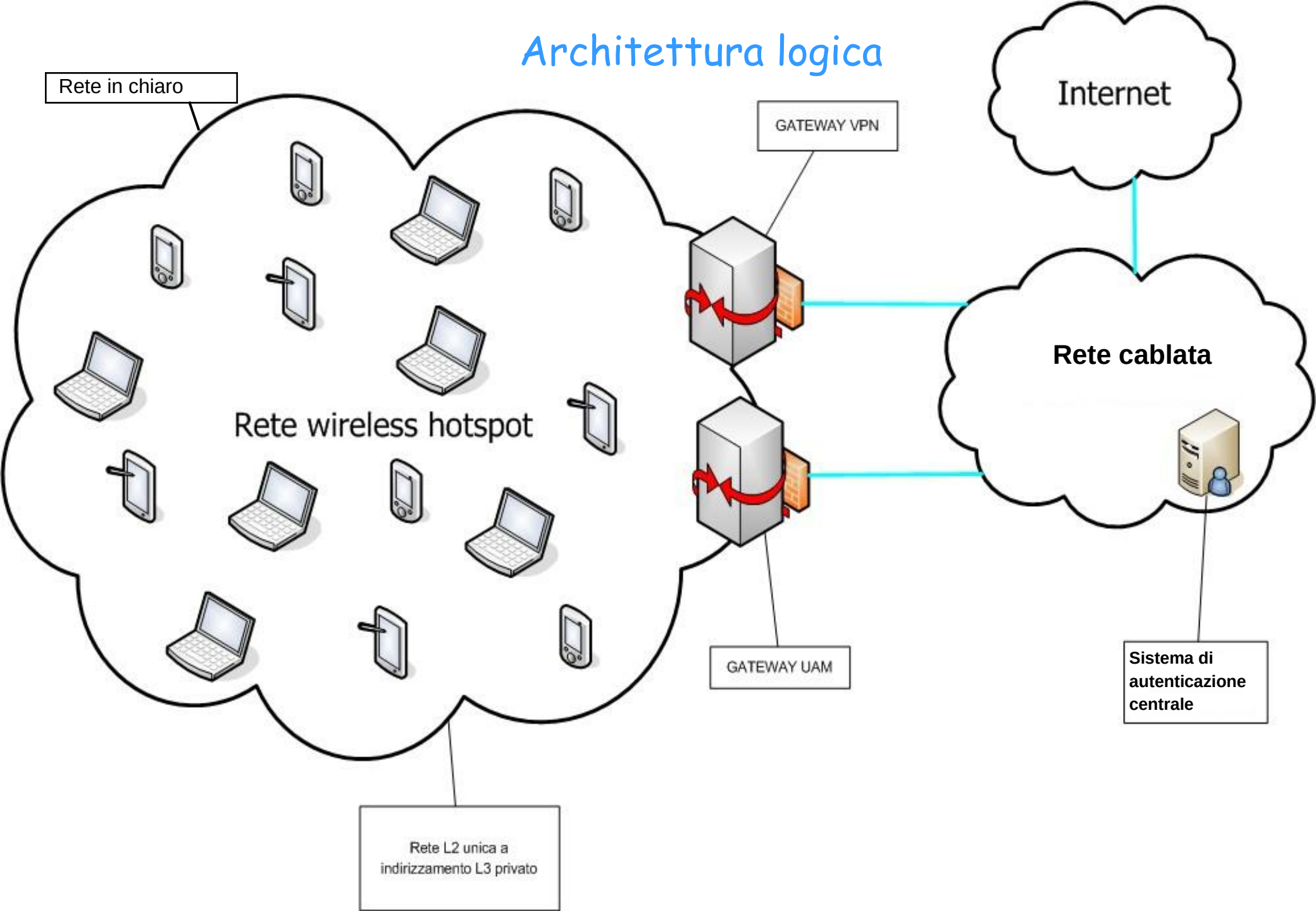
Agenda

- Esigenze e Requisiti
- Architettura
- Separazione servizi ed RF
- La Radio Frequenza
- Il sistema di AAA
- Sicurezza
- Politiche di firewalling
- La gestione degli utenti guest
- Scalabilità
- Monitoring
- Logging and Privacy
- Hardware e software
- Servizi utente
- Lan locali
- Statistiche

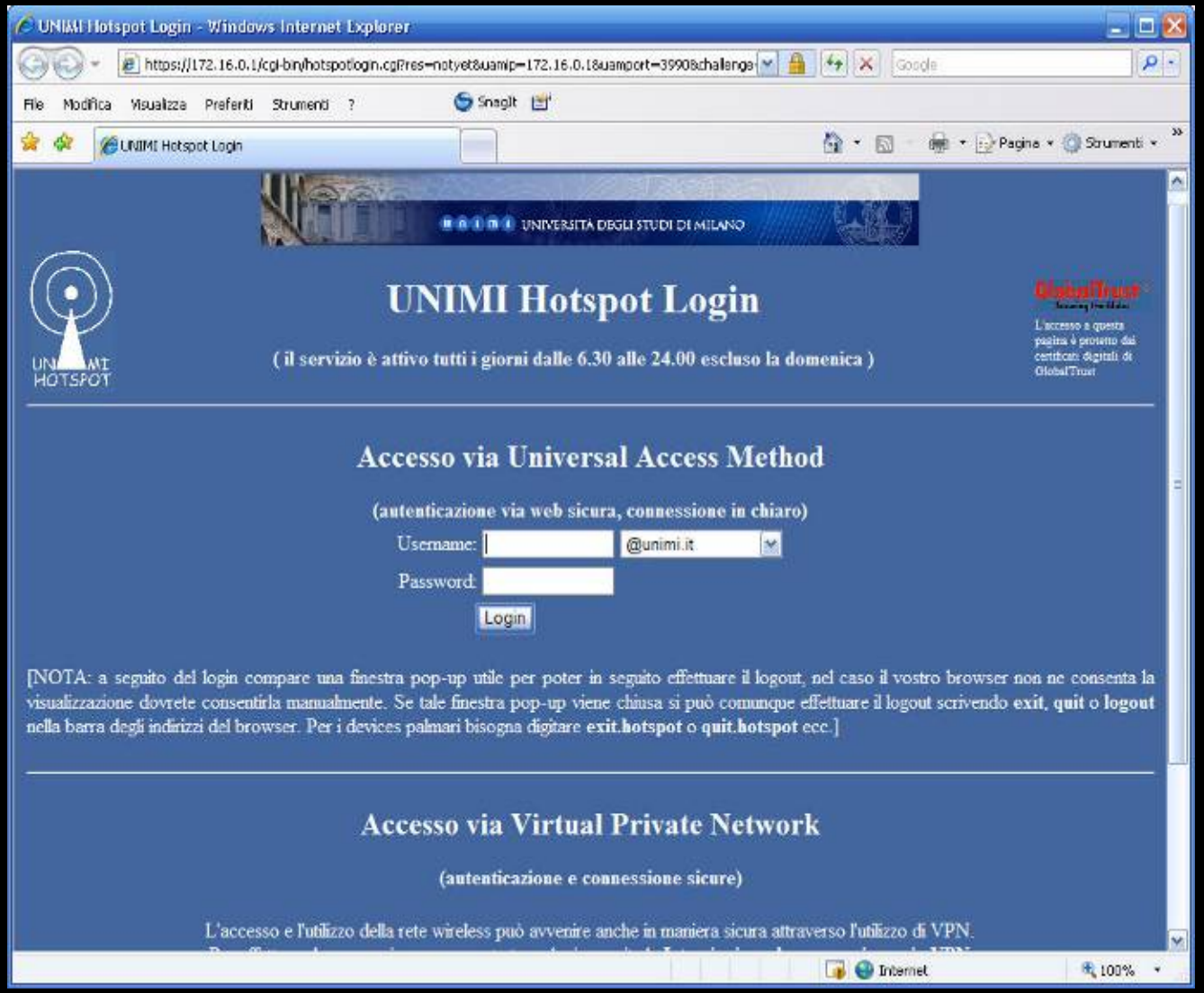
Esigenze e requisiti

- Facilità di uso
- Maggiore compatibilità possibile
- Mobilità
- Accesso ai servizi di ateneo
- Sicurezza
- Servizi indipendenti dal sistema RF
- Rispetto normative privacy
- Integrazione AAA

Architettura logica

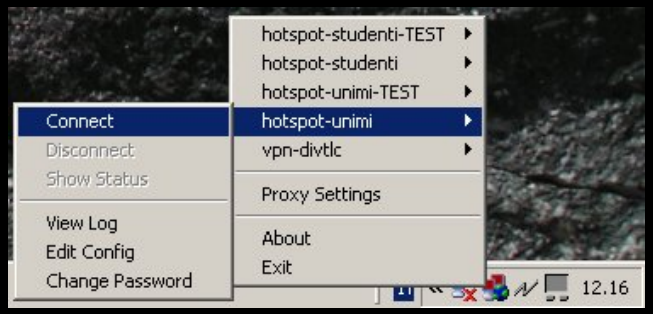


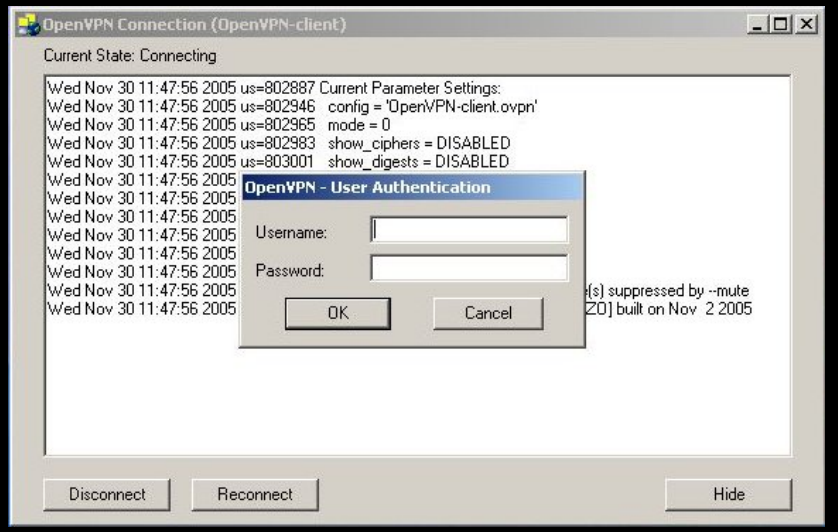
Screenshots portale web



Language sensitive

Screenshots VPN

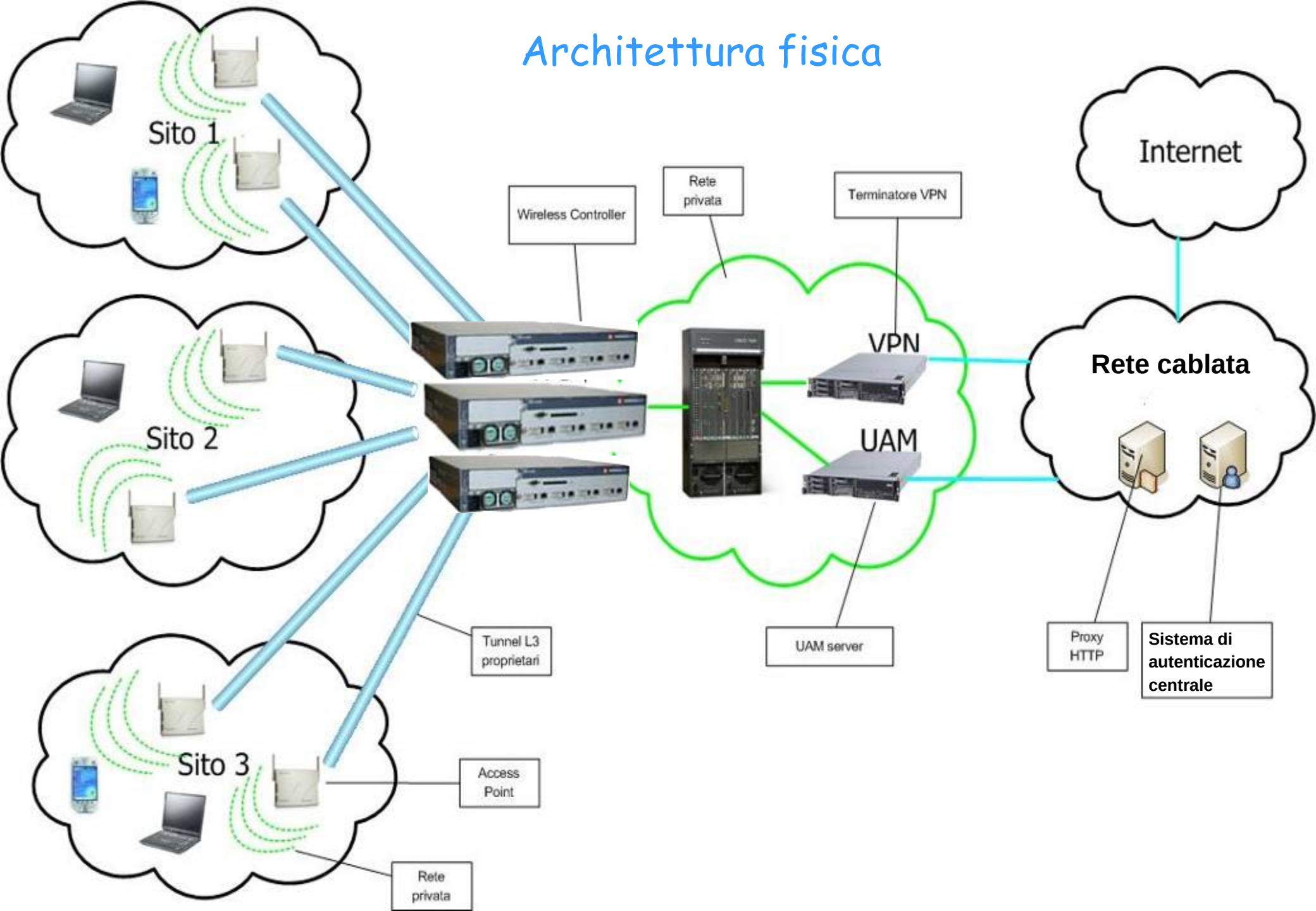


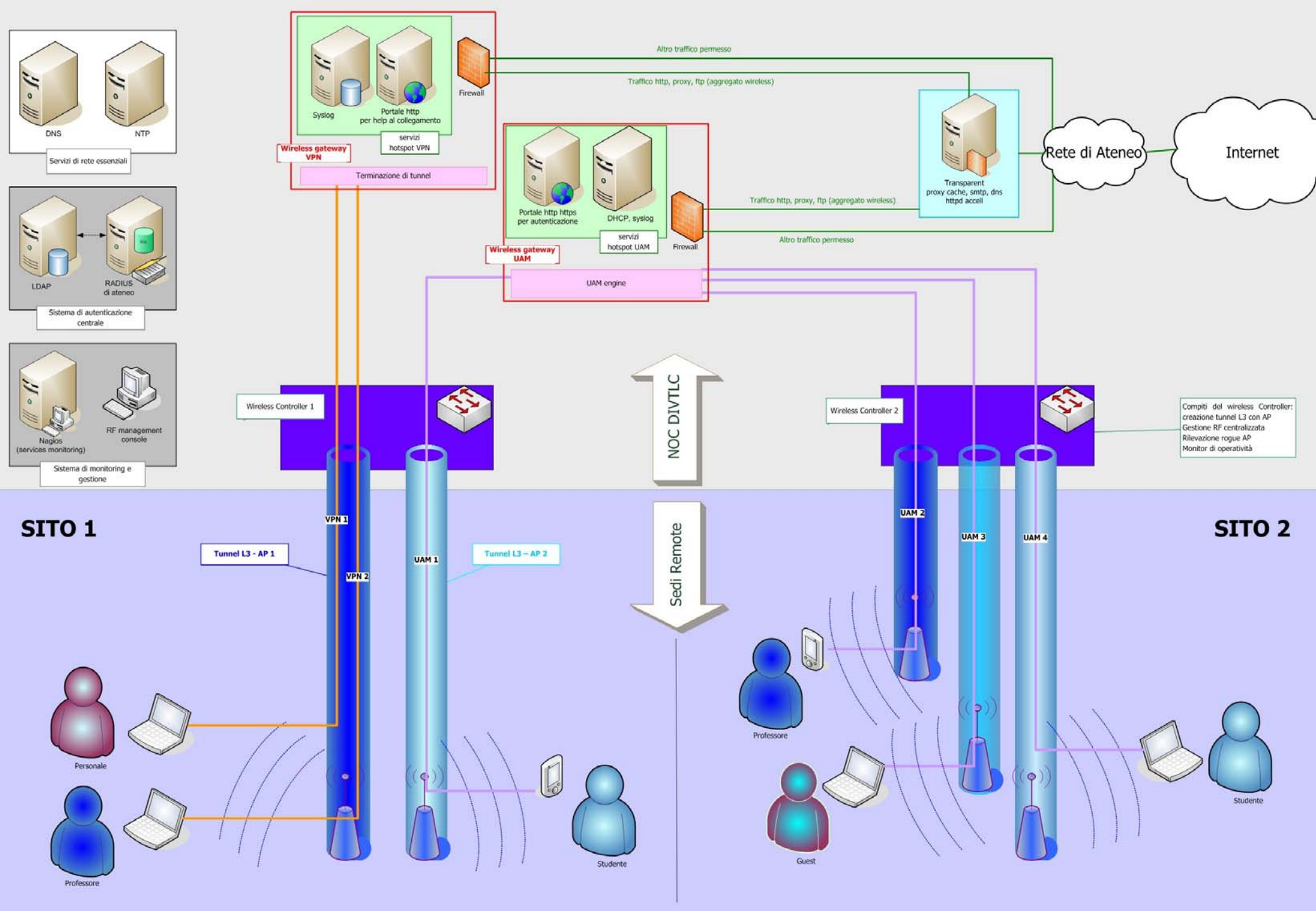


INDIRIZZAMENTO, SEPARAZIONE RETI E FLUSSI

- Separazione totale rete wireless / wired
- I gateway realizzano P-NAT
- Possibilità di limitazione banda di tutto il traffico hotspot

Architettura fisica




DNS
NTP
Servizi di rete essenziali
LDAP
RADIUS di ateneo
Sistema di autenticazione centrale
Nagios (services monitoring)
RF management console
Sistema di monitoring e gestione
Syslog
Portale http per help al collegamento
servizi hotspot VPN
Wireless gateway VPN
Terminazione di tunnel
Firewall
Altro traffico permesso
Traffico http, proxy, ftp (aggregato wireless)
Portale http https per autenticazione
DHCP, syslog
servizi hotspot UAM
Wireless gateway UAM
UAM engine
Firewall
Traffico http, proxy, ftp (aggregato wireless)
Altro traffico permesso
Transparent proxy cache, smtp, dns httpd accell
Rete di Ateneo
Internet
Wireless Controller 1
Wireless Controller 2
Compiti del wireless Controller:
creazione tunnel L3 con AP
Gestione RF centralizzata
Rilevazione rogue AP
Monitor di operatività
NOC DIVTLC
Sedi Remote
SITO 1
SITO 2
VPN 1
VPN 2
UAM 1
UAM 2
UAM 3
UAM 4
Tunnel L3 - AP 1
Tunnel L3 – AP 2
Personale
Professore
Studente
Professore
Guest
Studente

SEPARAZIONE SERVIZI ED RF

SISTEMA OPEN	SISTEMA PROPRIETARIO
AAA	GESTIONE RF
CAPTIVE PORTAL	TUNNELING L2
VPN	SNMP
FIREWALL	
PROXY	ALLARMISTICA
SYSLOG	

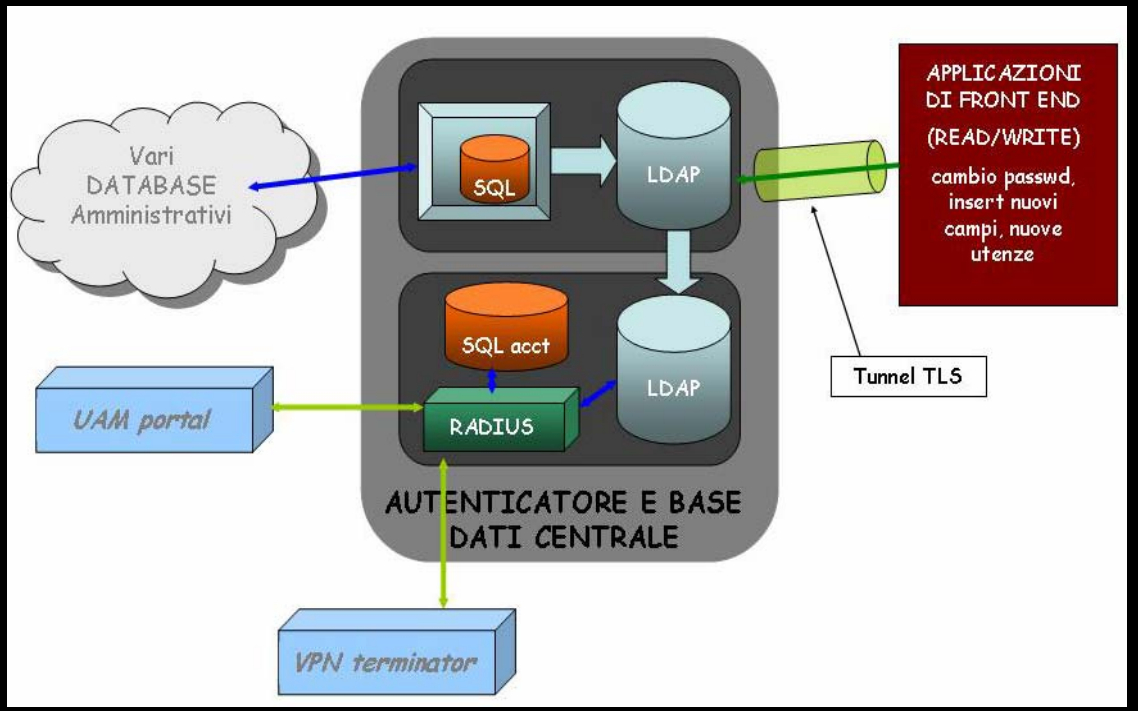
Radio Frequenza

Gli apparati di RF sono scelti per garantire:

- *User load balancing*
- *User isolation*
- *RF adattativa*
- *Easy AP deploy*

Il sistema di AAA

- L'autenticazione si appoggia al sistema centralizzato preesistente
- Autorizzazione dipendente da un flag di servizio
- Accounting su DB SQL utilizzato anche per statistiche e controllo degli accessi simultanei.
- Profilazione



Sicurezza (1)

- Separazione del traffico e dell'indirizzamento
- Accesso solo per utenti autenticati
- IP privato impedisce la fornitura di servizi accessibili dall'esterno
- Idle timeout
- Orario di operatività
- User isolation

Sicurezza (2)

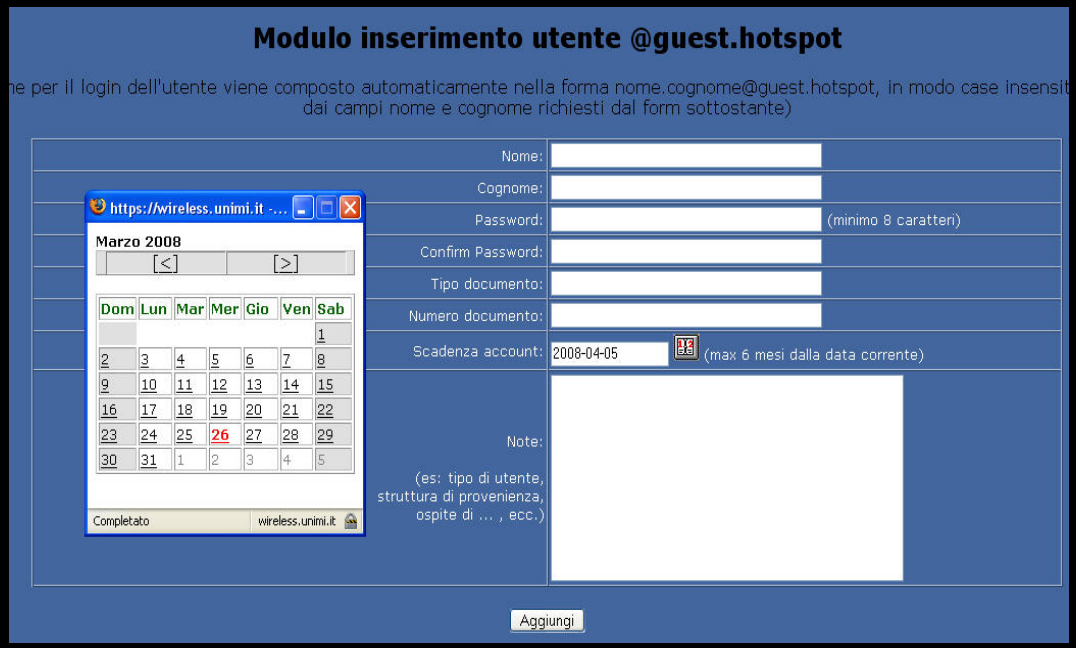
- Rilevazione tramite scansione RF dei rogue AP e relative contromisure
- Accesso sicuro tramite mutua autenticazione
- Possibilità di effettuare kick-off utenti
- Confidenzialità garantita per gli utenti in VPN
- Sensore ids che analizza il traffico wireless (autenticato e non)

Politiche di firewalling

- Il traffico viene filtrato dai gateway in funzione della politica di accesso definita per gli utenti wireless.
- Accesso UAM politiche restrittive ed uguali per tutti i soggetti che vi possono accedere.
- Accesso VPN meno restrittivo con profilazione delle regole in funzione della categoria di appartenenza.
- Traffico web è ridirezionato verso un proxy http (transparent proxy).
- Il traffico DNS/SMTP ridiretto verso i server di ateneo.

La gestione degli utenti guest

- Realm "@guest.hotspot" gestito da radius su DB separato
- Gestione decentralizzata attraverso una interfaccia web ssl per amministratori locali
- Sistema di cambio password per gli utenti guest



Scalabilità

L'architettura modulare:

RF

- basta aggiungere altri AP e altri Wireless Controller, questi ultimi dispongono di un protocollo per l'intercomunicazione e il roaming dei client

Servizi

- scalano con la potenza dei server che li ospitano. Ogni servizio può essere implementato su un server separato.
- Si possono eventualmente creare più isole hotspot identiche separate geograficamente

Monitoring

UTENTI

- Connessioni, durate, traffico (interim account ogni 4 minuti)
- Log (autenticazioni e tentativi, IP, MAC, username, connessioni http, traffico)
- Statistiche di utilizzo

RF

- Gestione centralizzata RF, allarmi, rogue AP detection

SERVIZI E RETE

- Monitor continuo dei servizi erogati (Nagios) con sistema di allarmi
- Console NOC monitoraggio rete

Logging & Privacy

- Prevista la conservazione dei dati di traffico anche in mancanza di una disciplina specifica delle tecniche di conservazione.
- I dati sono conservati limitatamente alle informazioni che consentono la tracciabilità degli accessi e delle connessioni, escludendo la conservazione del contenuto delle comunicazioni.
- E' possibile risalire all' attività in rete degli utenti ma al prezzo di molteplici correlazioni di informazioni presenti in differenti log e database posti su apparecchiature diverse e gestiti da incaricati diversi.

Hardware e software

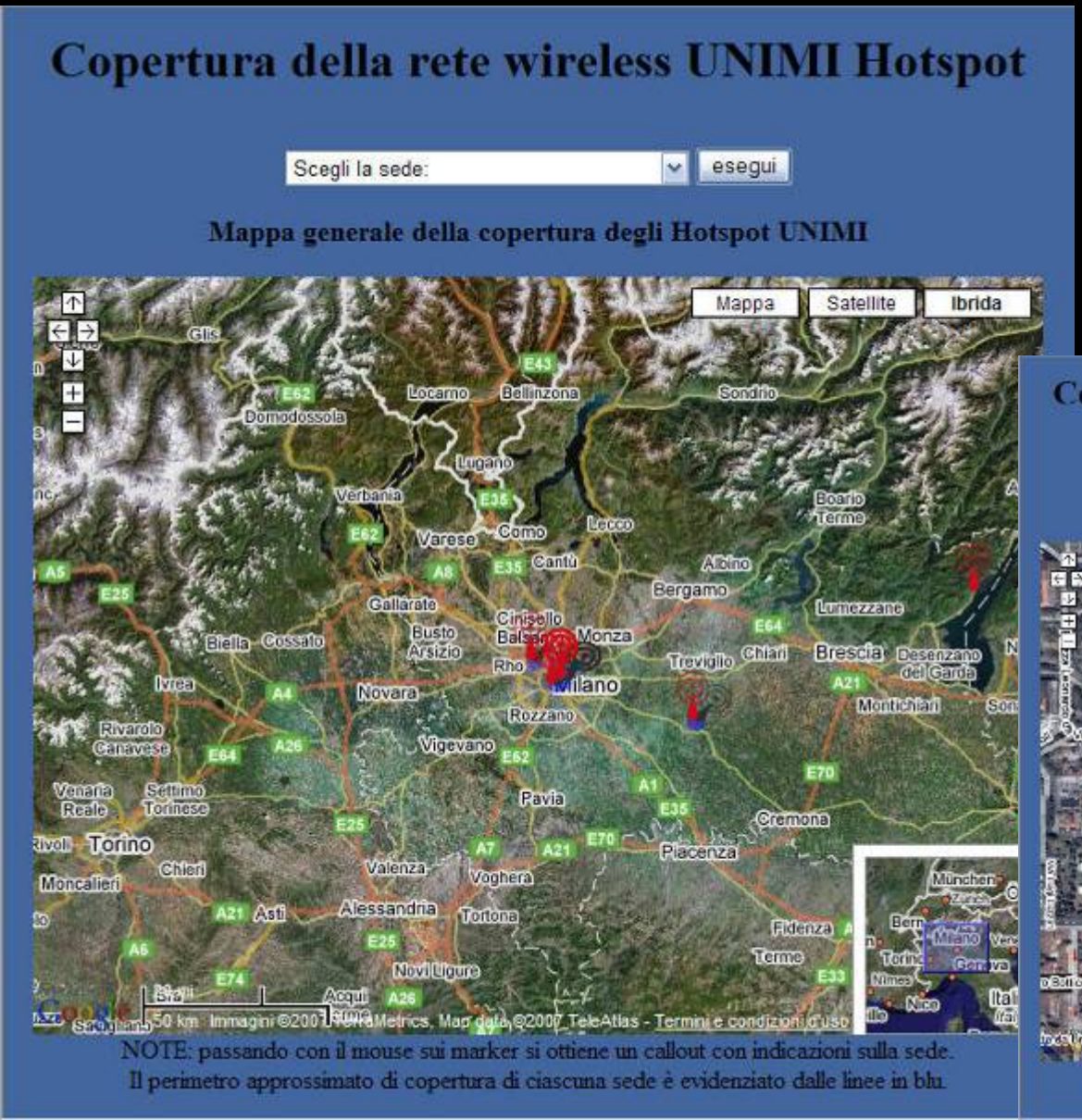
HARDWARE

- Server Rack overprovisioned
- 3 Wireless Controller con doppia alimentazione
- Dischi e alimentazioni ridondate
- Posizionamento in sala macchine con ups e condizionatore
- Manutezione (e backup periodico di tutto il sistema)

SOFTWARE

- Il software per la realizzazione dei servizi è tutto Open Source o sviluppato in proprio
- Il software per la gestione della Radio Frequenza è proprietario

Mappe informative sulla copertura



Attraverso le API di google maps si sono realizzate mappe che forniscono i perimetri di copertura della rete hotspot sul territorio

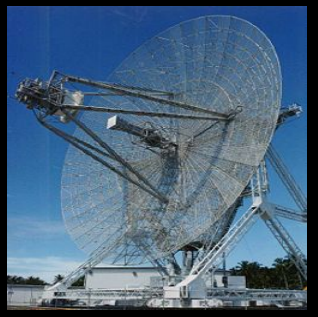
Localizzazione

- Rende visibile una Google Map che mostra all'utente su quale AP è collegato e una copertura di massima
- Vengono visualizzati i servizi disponibili in quella determinata zona sotto forma di url create dinamicamente

Connessioni alle LAN locali

- Attraverso dei server VPN locali in "white list"

- Utilizzando degli AP di nuova generazione (in fase di test)



Statistiche

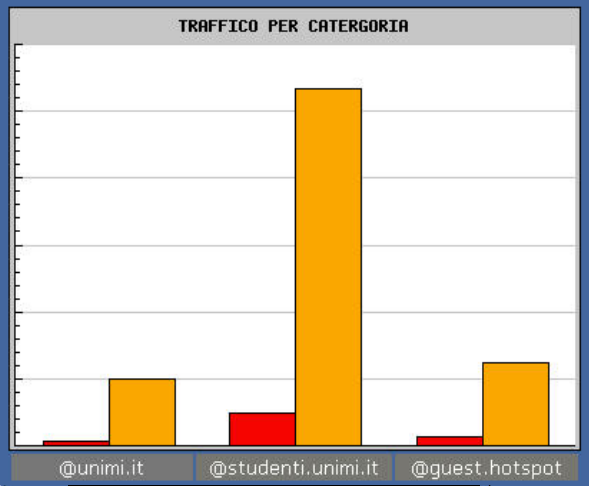
Hotspot wireless
Pagina di statistiche & management utenti

Statistiche				
Utenti attualmente autenticati				esegui
Utenti connessi suddivisi per sede				esegui
Utenti Guest presenti nel DB				esegui
Grafico tipologie di utenti dal	02/04/2008	al	02/04/2008	esegui
Istogramma traffico utenti dal	02/04/2008	al	02/04/2008	esegui
Traffico generato dagli utenti dal	02/04/2008	al	02/04/2008	esegui
Numero accessi effettuati dal	02/04/2008	al	02/04/2008	esegui
Causa di terminazione delle sessioni dal	02/04/2008	al	02/04/2008	esegui
Medie sui tempi di connessione e traffico dal	02/04/2008	al	02/04/2008	esegui
Metodo di accesso per tipologie di utenti dal	02/04/2008	al	02/04/2008	esegui
Management utenti				
kickoff immediato ma temporaneo utenti attualmente connessi				esegui
kickoff immediato e definitivo utenti attualmente connessi				esegui
kickoff definitivo utente		@unimi.it		esegui
Riammissione utente		@unimi.it		esegui

NB: tutte le date sono nel formato gg/mm/aaaa

Istogrammi dei volumi di traffico suddivisi per tipologie di utenti dal giorno 01/04/2008 al 02/04/2008:

REALM	TRAFFICO IN	TRAFFICO OUT
@unimi.it	271.27 MB	4.63 GB
@studenti.unimi.it	2.26 GB	24.86 GB
@guest.hotspot	596.4 MB	5.8 GB



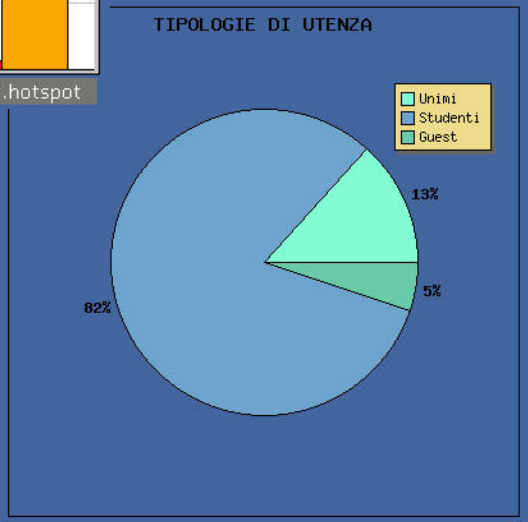
Cause della terminazione delle sessioni utente dal giorno 01/09/2006 al 02/04/2008:

TERMINATE CAUSE	NUMERO EVENTI
Lost-Carrier	75601
User-Request	25941
Vpn-Disconnect	11770
Idle-Timeout	6702
NAS-Reboot	146
Admin-Reset	95

o delle perce gie di utenti /2006 al 02

iche sono calcolate
nti che hanno utiliz
ichiesto

REALM	NUMERO UTENTI
@unimi.it	982
denti.unimi.it	6020
est.hotspot	374



GRAZIE!

Michele.devarda@unimi.it